Anno 3 – N. 59
23 settembre 2004 - 7 ottobre 2004

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Boss: TheGuilty@hackerjournal.it

I Ragazzi della redazione europea:
Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron Silvio De Pecher, Contents by MDR

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Direttore Responsabile: Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Musica per le **orecchie di tutti**

Niente batte l'estate e le vacanze, ma c'è bello anche nell'autunno che arriva. Hai questa sensazione che tutto ricominci e che possano accadere cose decisive, importanti. Cose che finalmente possiamo ricominciare ad affrontare con un iPod (o equivalente) in tasca, perché tornano le tasche, insieme ai vestiti, e perché se c'è musica siamo tutti più bravi. E anche un po' più buoni.

È proprio sulla musica che sono già successe cose importanti e decisive. Prima: DVD Jon ne ha fatta un'altra delle sue. Non gli bastava il crack della codifica dei DVD e adesso si è dedicato ad AirPort Express, la base wireless con l'uscita audio. Fino a che non ci si è messo Jon si poteva mandare musica su AirPort Express solo con iTunes; ora, grazie alla sua bravura, lo potranno fare tutti. La notizia è più simbolica che altro, ma sono simboli che ci piacciono. Novità che suonano bene.

Ma la notizia più importante, per restare in... tema, è la sentenza sul P2P. I produttori del software non sono responsabili dell'uso che ne fanno gli utenti. Sembra una cosa normale, che capisce anche la nonna. Ma non è così. Fino a ieri i discografici sostenevano il contrario. Se compri un CD audio e con quello uccidi qualcuno siamo colpevoli anche noi, dicevano, in pratica. È una posizione talmente stonata che non meriterebbe neanche un commento. Finalmente hanno torto. Finalmente hanno torto quelli con i soldi.

Sono avvenimenti ideali per chiudere bene l'estate e aprire ancora meglio l'anno che ci aspetta. Non c'è da abbassare la guardia però. Sarà un anno fatto di decreti Urbani, di virus intelligenti scritti da idioti.

Noi potremmo farne un anno diverso. Dodici mesi di condivisione delle conoscenze. Di scoperte affascinanti. Di curiosità, ingegno teorico e applicato. Di progressi, di espansione delle nostre capacità. Di occhi e orecchie bene aperti e vigili come non mai, per difendere la nostra libertà. Quelli che hanno i soldi il potere lo comprano. Quelli come noi il potere lo ottengono attraverso la conoscenza. Potere che non serve a dominare, o a fare il male, ma a proteggerci da chi vuole approfittare di noi e della rete.

Dodici mesi di conoscenza, occhi aperti, e tanta musica che da ieri è un pochino più libera. Lo diventerà sempre di più. Sarà una lotta dura. Ma alla fine è la libertà, che vince. E noi ci saremo. Appuntamento, tutti, nessuno escluso, ogni due settimane per fare il punto. E portiamo gli amici, che devono sapere anche loro.

theguilty@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Sarà Service? OCCHIO al Pack!

Se SP2 in italiano avrà gli stessi problemi di quello inglese, meglio andarci cauti

Siamo agli sgoccioli: il Service Pack 2 in italiano per Windows è appena uscito, o sta per uscire. Ma in tutti i casi è consigliabile attendere che le acque si calmino, prima di mettersi a scaricarlo.
La versione americana, infatti, era tutt'altro che perfetta e Microsoft ha già provveduto, come in passato, a preparare altre patch da applicare alla patch.

Altra cosa da ricordare, bisogna essere in regola con Microsoft. Esattamente come il Service Pack1, anche SP2 controlla la validità della ID del prodotto (PID) e, se a Microsoft non piace quello che si vede, l'aggiornamento non si installa. Pare, si dice, che SP2 dia per non validi tutti i PID privi della stringa 640, ma non è un dato certo e bisognerà verificare la cosa quando avremo in mano il software.

Una grande patch che richiederà altre patch!

Sicurezza, sicurezza, sicurezza. Ma c'è il bug

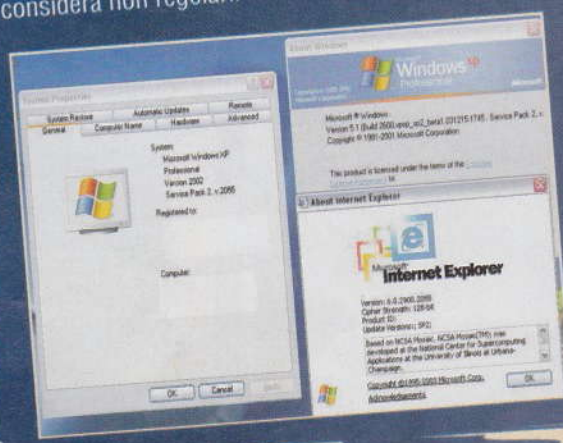
Service Pack 2 in realtà è una buona cosa, che ha lo scopo di rendere Windows un po' più sicuro del colabrodo attuale. La maggioranza del codice presente nell'aggiornamento tappa buchi, sistema problemi e dà più disciplina a tutto il sistema. Per fare un esempio, Internet Explorer non è stato in alcun modo potenziato o aggiornato. Tanto per dirne una, manca ancora la navigazione via tab, che c'è in tutti gli altri browser da Mozilla in giù ed è tanto comoda. Ma i popup pubblicitari ora vengono disattivati automaticamente, mentre prima non lo erano e costituivano un ennesimo rischio di sicurezza.

Come al solito, però, ci sono tante buone intenzioni e qualche inciampo. Sempre in Internet Explorer, tanto per dire, è possibile bucare la chiusura della Security Zone. L'uso di un valore non convenzionale nel campo Content-Location di un file MHTML (MIME HTML) fa sì che il browser esegua il file nella zona della Intranet locale e non limitatamente al singolo computer. Così diventa possibile fare andare script che altrimenti non verrebbero autorizzati eccetera eccetera. Non è una falla grave; ma ce ne sono un sacco di altre. Service Pack 2 rende Windows più sicuro, ma non lo rende sicuro.

Parleremo più estesamente di SP2 nei prossimi numeri di Hacker Journal. Nel frattempo, come sempre, fate attenzione. SP2, in fatto di sicurezza, non sostituisce (e non ferma vista dall'altro lato) un hacker sveglio.

Barg the Gnoll
gnoll@hackerjournal.it

COME GUARDARSI IL PID

Per sapere qual è il PID della nostra versione di Windows dobbiamo fare clic con il tasto destro del mouse su Risorse del Computer, Proprietà, Registrato a nome di:. Pare che Service Pack 2 farà lo schizzinoso e non si installerà sui sistemi che considera non regolari.

◄ Service Pack 2 sta arrivando. Installiamo senza fretta e con attenzio

HOT!

I SIGNORI IN GIALLO E GLI SMS

Ogni SMS spedito da un cellulare cinese sarà controllato e il suo contenuto verrà filtrato per vedere se ci sono riferimenti a pornografia o altri reati. Ma Reporter Sans Frontières denuncia l'abuso di questo controllo da parte del governo cinese, che ne approfitta per tenere sotto controllo i potenziali dissidenti. Il sistema sarebbe in grado di lanciare un allarme automatico alla polizia quando individua una parola sospetta e archiviare tutti i messaggi spediti da numeri sotto sorveglianza specifica. In Cina circolano già 300 miliardi di SMS l'anno.

TROPPE RICARICHE?

A una donna di Povegliano, provincia di Treviso, è scoppiato il cellulare, un Nokia 3310. Pare che il telefono fosse sotto carica ma che il chip incaricato di interrompere la carica a batteria piena non abbia funzionato, portando al surriscaldamento e all'esplosione. La donna se l'è cavata con sei punti di sutura alla mano e il figlio, che si trovava nelle vicinanze, con qualche graffio alle gambe. Chissà se la mamma lo rimprovererà ancora di usare troppo il cellulare...

AUTO VOLANTI TRA DIECI ANNI?

Secondo un'inchiesta pubblicata dal settimanale Businessweek potremmo avere auto volanti entro non più di dieci o vent'anni. Honda e Toyota starebbero già sviluppando prototipi di apparecchi volanti a uso personale e General Electric sarebbe al lavoro su un modello di jet come quelli in uso sugli aerei, solo più piccolo e adatto a un veicolo della taglia di un'auto.

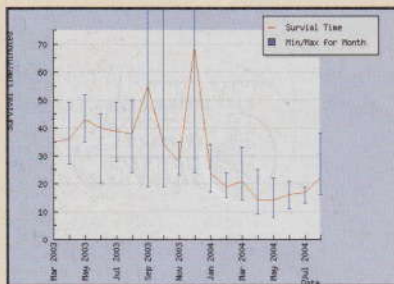
Nell'attesa di emulare Bruce Willis, tassista a tre dimensioni del film Il quinto elemento, attendiamo con ansia il momento in cui le autostrade non sapranno come fare pagare i loro pedaggi.

LINUX NON ESISTE, DICE SCO

Kieran O'Shaughnessy, direttore di SCO per Australia e Nuova Zelanda, ha dichiarato che "Unix non esiste. Tutti sanno che Linux è solo una versione senza licenza di Unix", in un'intervista a LinuxWorld.com.au. Come è noto SCO ha lanciato una guerra legale contro Linux accusando il sistema di violare tutta una serie di brevetti e, sostanzialmente, chiedendo soldi alle aziende che usano Linux in cambio di tranquillità legale. Sullo sfondo della battaglia l'andamento di SCO, che nel 1999 incassava 250 milioni di dollari l'anno e adesso ne incassa 40. Ovvio che il software libero a loro dia fastidio e che dietro, come al solito, ci sia lo zampino di Microsoft.

POVERE CASE DISCOGRAFICHE

Un'autorevole fonte inglese, http://arstechnica.com/news/posts/20040903-4156.html, riporta il fatto che a dispetto delle lacrime versate dalle case discografiche e delle conseguenti leggi emanate dai paesi europei per tentare di abbattere il p2p, le stesse case denunciano profitti record, mai visti prima. BMI, per esempio, che tanto si è lamentata di perdite inimmaginabili causate dallo scambio di file tra studenti e privati, a guardare bene denuncia incrementi di fatturato pari al 6,8%, per qualcosa come 43 milioni di dollari in più dell'anno passato. Con royalty conseguenti distribuite agli autori. Il boss di BMI ha dichiarato perfino che è la "più grande distribuzione di diritti nella storia dell'azienda". Alla faccia delle lacrime, di coccodrillo, per il p2p.

QUATTORDICI MINUTI AL CONTAGIO

L'Internet Storm Center (http://isc.sans.org) monitorizza costantemente il tempo medio di sopravvivenza di un PC Windows su Internet. Ossia installano un PC così come esce dalla scatola, lo attaccano a Internet senza fare nient'altro che aspettare e vedono in quanto tempo il PC si becca un virus o un worm. Se a marzo 2003 il tempo medio di sopravvivenza era di 35 minuti, adesso è intorno ai venti! Nel momento in cui il tempo di sopravvivenza è minore del tempo necessario a caricare le patch e gli aggiornamenti di sicurezza del sistema, si creano grossi problemi, perché è impossibile proteggere il sistema (senza hardware aggiuntivo) prima che venga compromesso. Usando altri sistemi operativi, come Linux o Mac OS X, il tempo di sopravvivenza è infinitamente più lungo...

283 BREVETTI, SARÀ LUNGHETTA

Secondo la società Open Source Risk Management (http://www. osriskmanagement.com) sarebbero 283 i brevetti che Linux rischia di violare e che potrebbero portare a cause legali anche problematiche.
Il problema dei brevetti esiste, perché – detto in due parole – gli uffici che li gestiscono non capiscono niente di tecnologia e chiunque può lavorarci un po' sopra e poi provare a brevettare la ruota o il tasto asterisco del cellulare. Ma la situazione non è grave come appare dai numeri: di questi brevetti, Microsoft (l'unica vera nemica dell'open source) ne possiede meno di trenta e gli altri sono in mano a società che lavorano anche su Linux, come IBM o HP. E poi OSRM vende risk mitigation and management solutions: in pratica, assicurazioni per le aziende che usano Linux. Hanno tutto l'interesse ad alzare un po' di polverone.

U2 E RETE: BONO COSÌ?

Alla fine non succederà niente di speciale. Durante una sessione dal fotografo, gli U2 avevano smarrito un CD contenente i brani del loro prossimo album, di cui non si sapeva niente. Il leader Bono aveva accennato alla possibilità di rilasciare l'album in anteprima sull'iTunes Music Store nel caso che i brani avessero iniziato a girare per Internet. Pochi giorni fa, le conferme: l'album uscirà il 22 novembre e il primo singolo, nelle radio dal 24 settembre, uscirà l'8 novembre. E il CD sparito, il pericolo del P2P? Resta il dubbio che fosse soltanto pubblicità...

HOT!

FOTORITOCCO CHE SCOTTA

Alla Dartmouth University degli USA stanno lavorano a software, presentato nel corso del Workshop on Information Hiding di Toronto, Canada, in grado di riconoscere le immagini digitali che sono state sottoposte a fotoritocco. Scene di panico tra le attrici da calendario. :-)

VIRUS A QUOTA 64

Benvenuto, per modo di dire, a Shruggle, alias W64. Shruggle.1318, il primo virus capace di infettare sistemi a 64 bit. Per la precisione l'animale è il primo a poter attaccare file eseguibili Windows a 64 bit su sistemi AMD64. In sé la minaccia è di poco conto, perché il virus non è neanche capace di autopropagarsi ed è solo una proof of concept. Ma dimostra la capacità degli sviluppatori di codice malevolo di attaccare qualsiasi piattaforma Windows.

PROXYMAMENTE A 56K

Da pochi giorni ho deciso di provare a navigare attraverso server proxy. Ho configurato il browser di navigazione (IE 5.50) attivando la casella "utilizza un server proxy" e immettendo l'indirizzo del server e la sua porta d'accesso, ho provato anche ad usare la tecnica del multiproxy, ma non riesco a navigare; è il mio 56K che non regge, oppure c'e qualche sbaglio di configurazione, o non è possibile farlo?

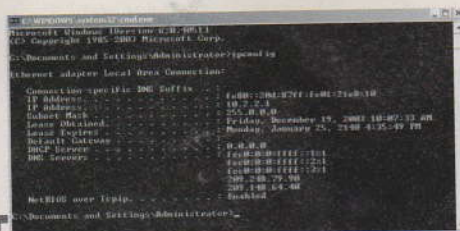
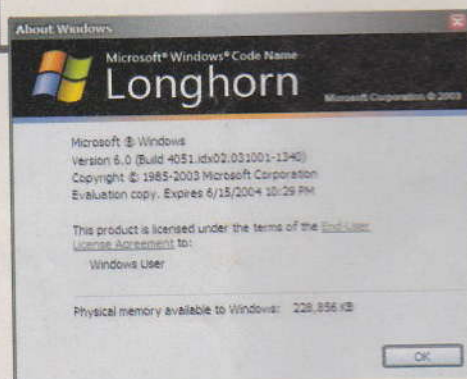
C1P8

Per ogni proxy che aggiungi la connessione viene rallentata quindi, se il problema è questo, è tutto normale. Verifica i proxy collegandotici con telnet. I casi sono tre: non si connette (vecchio e non funziona più), si connette ma perde contatto dopo qualche secondo (lascialo perdere) oppure resta collegato (ok). Attenzione a scegliere proxy adeguati. Per andare a newsgroup te ne serve uno vicino a casa; se invece devi sbrigare faccende delicate è meglio usarne uno remoto, remotissimo, anche se meno performante. In tutti i casi, ricorda che non sei mai perfettamente anonimo! Considera inoltre la possibilità di risolvere il problema passando da posti come http://www.anonymizer.com.

START, ESEGUI, ARTICOLO

Perché non parlare in un prossimo articolo di tutte quelle funzioni di Windows attivabili da Start\Esegui come per esempio netsend, dxdiag, winver e il famosissimo regedit?

Andrea

È che sono infinite! Qualunque utility MS-DOS può essere fatta partire da Start\Esegui e su Internet ce ne sono squinzilioni. In questo numero trovi cose interessanti su diskperf, mentre di netsend abbiamo già detto qualche numero fa... un po' alla volta sveleremo tutti i segreti del DOS!

SPECIALI WML

Ciao Reed Wright, ho letto il tuo articolo su WML, volevo chiederti se puoi inviarmi un esempio in WML su come inserire i caratteri speciali.

Luciano

Ciao Luciano!
I caratteri speciali in WML funzionano in modo estremamente simile a quelli in HTML, ossia richiedono codici altrettanto speciali.
Per vedere qualche uso pratico, prova ad andare (solo alcuni degli infiniti esempi possibili) http://www.javacommerce.com/tutorial/wap/wap5.htm, http://webmaster.spray.se/topics/technic/wap/wap-workshop1/4/ o http://www.softsteel.co.uk/tutorials/wmltut/append.html. Eccezione interessante, il segno di dollaro: $. In WML si scrive $$. Dimenticavo: i codici possono essere inseriti con i loro nomi (>), oppure come numeri decimali (>) oppure ancora come esadecimali (>). Prova una prima paginetta così:

```
<card id="codici">
<p>
e_commerciale = &amp; <br/>
apice = &quot; <br/>
minore = &lt; <br/>
</p>
</card>
```

Reed Wright
reedwright.mail.inet.it

CARATTERI SPECIALI IN WML

&	&
"	"
'	'
<	<
>	>
Spazio non divisibile	

DOPPIO BROWSER

Possiamo testare le nostre pagine WML a http://www.wapsilon.com/main.html, dove ci sono sia un browser WML, sia la conversione automatica in HTML del nostro codice, così che lo possiamo anche guardare con un browser qualunque, su un normale computer.

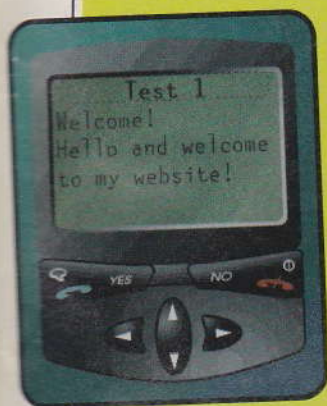
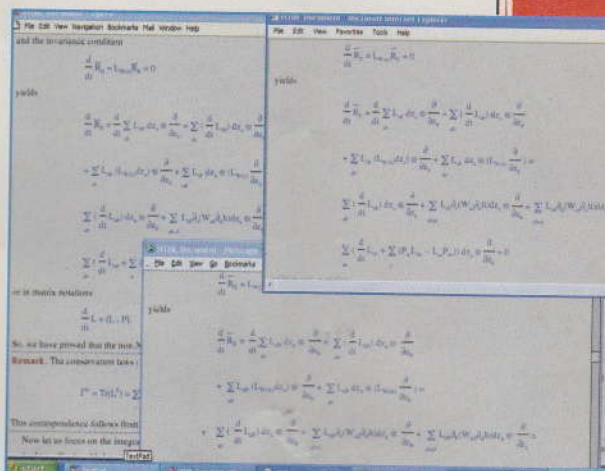
HTML IMPARASI

Ho intenzione di farmi un sito e vorrei sapere che differenza c'è a farlo con programmi tipo FrontPage o con un editor di testo in formato HTML. Premetto che ne so poco o nulla di programmazione; mi potete indicare un editor di testo per fare il mio sito e anche un libro per imparare a programmare in HTML?

Vale 87

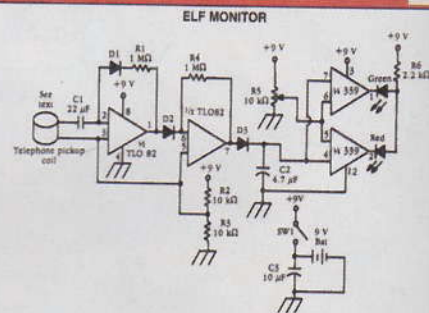
Con FrontPage lo fai in fretta, perché il programma ti mostra subito a video come apparirà più o meno la pagina, ma la qualità del codice sarà scadente (FrontPage è uno dei peggiori editor HTML che esistono). Ossia ci saranno problemi di compatibilità, le pagine peseranno più del necessario (e quindi si scaricheranno con più fatica) e in condizioni particolari potrebbe essere impossibile usare il sito.
Con un editor di testo inizi in modo più difficile, perché non hai la visione di insieme delle pagine, ma

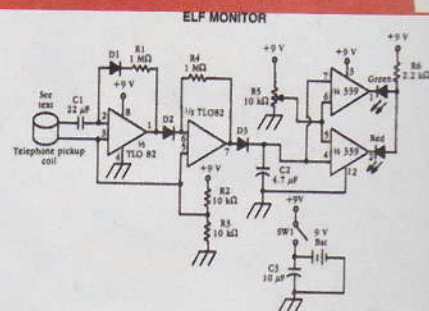
il codice è più pulito ed efficiente. Ti consigliamo di lavorare in testo. Fai più fatica, ma se c'è un errore impari a capire dove sta e a correggerlo, e il tuo codice sarà molto più pulito. Per imparare l'HTML, niente libri. Sono fermi, il Web è dinamico invece. Guarda il codice delle pagine che ti piacciono e ruba i loro segreti! E poi studia su http://basic.html.it.

Trattino di sillabazione	
$	$$
à	à
é	é
è	è
ù	ù
ç	ç

ASCOLTO INASPETTATO

L'altro giorno stavo ascoltando un CD sul mio computer con le cuffie collegate a una cassa. Tutto d'un tratto ho interrotto volutamente la riproduzione e dalle cuffie si potevano sentire come sottofondo delle voci in lingua inglese. Come è possibile tutto ciò? Non può essere il CD perché la riproduzione era interrotta. Vi prego, datemi una spiegazione.

:spy23:.

Il tuo apparato, dal computer fino alle casse, si è momentaneamente trasformato in un ricevitore di segnali radio. Succede più spesso di quello che si pensa, solo che non ci facciamo attenzione e normalmente il segnale è molto debole. Hai captato una stazione straniera, o una conversazione tra radioamatori, o chissà. Complotti spionistici? Difficile, ma chi può escluderlo? :-)

A telephone pick-up coil is used as a sensor for low-frequency magnetic fields. The signal ... plified and detected, then used to drive a comparator.

▲ *Un telefono può diventare sensore di campi magnetici.*

A telephone pick-up coil is used as a sensor for low-frequency magnetic fields. The signal ... plified and detected, then used to drive a comparator.

▲ *Registrare una telefonata? Basta davvero poco...*

Blogghiamo con una marcia in più!

L'hacker si vede anche nelle piccole cose. A mettere in piedi un blog ci vuole niente. A farne uno perfetto e pienamente accessibile ci vuole qualche trucco

L'informazione nascosta, da hacker dà un po' fastidio. L'informazione deve essere libera. Ma quando facciamo pagine Web che qualcuno non può leggere nascondiamo informazione, non importa se a pochi o a tanti. Internet è un mezzo universale, non di massa. Chiunque ha il diritto di leggere una pagina Web e chi le scrive ha anche un dovere, per quanto morale, di consentirglielo.
I consigli che seguono sono pensati per il nostro blog (abbiamo un blog, vero? Altrimenti, che cosa aspettiamo a farlo e segnalarlo ad HJ?). Ma in realtà valgono per qualunque sito vogliamo mettere in opera.

Giochiamo al doctype

Così come in italiano una frase inizia con la maiuscola, in HTMl si inizia con un doctype. Certo se ne può fare a meno, ma è cattivo scrivere, in tutti e due i casi. Può darsi che abbiamo già un doctype nel documento; nel caso, si trova sicuramente all'inizio del codice.

Un buon parametro da usare come doctype è XHTML 1.0 Transitional. È quello che impiega il template di default di Movable Type, per esempio. Radio Userland, Manila e Blogger usano tipicamente HTML 4.01 Transitional, che va bene anche lui. Altri doctype ugualmente buoni sono HTML 4.01 Strict, XHTML 1.0 Strict e XHTML 1.1.

Chi ha un template con dentro un doctype già fatto molto probabilmente può lasciarlo com'è. Chi non ha un doctype farebbe bene ad aggiungerne uno come questo:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
```

Se, aggiungendo il doctype, cambia qualcosa nella resa a video delle pagine, si può provare la via del compromesso e scegliere un doctype a metà, tipo questo:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
```

Naturalmente, ogni pagina deve avere il suo bel tag doctype. Parlando di blog e di sistemi di blog, questi sono i template migliori da usare sui vari sistemi (chi vuole farsi il suo template è liberissimo!). Ricordiamoci di controllare ed eventualmente sistemare il doctype.

- **Movable Type:** Main Index, Master Archive Index, Category Archive, Date-Based Archive e Individual Entry Archive;
- **Radio Userland e Manila:** Main Template e Home Page Template;
- **Greymatter:** Main Index-Related Templates, Archive-Related Templates e Entry-Related Templates;
- **Blogger:** più complicato. Nel main template di Blogger andrà probabilmente inserito a mano un doctype. Se l'Archive Template di Blogger è una pagina a parte (nel senso che ha un suo tag <html>), va aggiunto il doctype anche lì.

Cosa importante: la scelta del doctype influenzerà anche le altre decisioni di programmazione del codice di un blog. O di qualunque altra pagina Web. Nei prossimi articoli prenderemo varie decisioni su molti aspetti della programmazione di un blog e arriveremo a offrire una accessibilità davvero superiore. Chi ha un blog ce lo faccia sapere. Li guardiamo tutti!

P. Greco
p.greco@hackerjournal.it

Piattaforme di blog

Movable Type - http://movabletype.org
Greymatter - http://www.noahgrey.com/greysoft/
Blogger - http://www.blogger.com
Splinder - http://www.splinder.it
Userland - http://www.userland.com
Manila - http://www.userland.com

Accessibile perché

Gianna ha perso la vista da otto anni e naviga sul Web usando Jaws (http://www.freedomscientific.com/fs_products/software_jaws.asp), un sintetizzatore vocale che legge le parole che compaiono a video. Anche siti molto complessi sono navigabili con profitto, a patto che sotto il cofano siano realizzati in modo leggibile.
Michele soffre di acromatopsia, o daltonismo, ossia vede il mondo in toni di grigio. Inoltre ha una connessione 56K che spesso dà persino meno banda della poca promessa. Molto spesso naviga usando Lynx (http://lynx.browser.org), il browser solo testo, oppure Opera, che carica le pagine in background e permette di disabilitare facilmente la visualizzazione delle immagini. Sono solo due degli esempi possibili di persone per le quali l'accessibilità di un sito, di qualunque sito, è un must.

...LESS PUBLISHING
JOURNALS + E-PORTFOLIOS
NOTHING CAN STOP IT!!
THE BLOG

l'informazione deve essere libera
Facciamo pagine Web per tutti

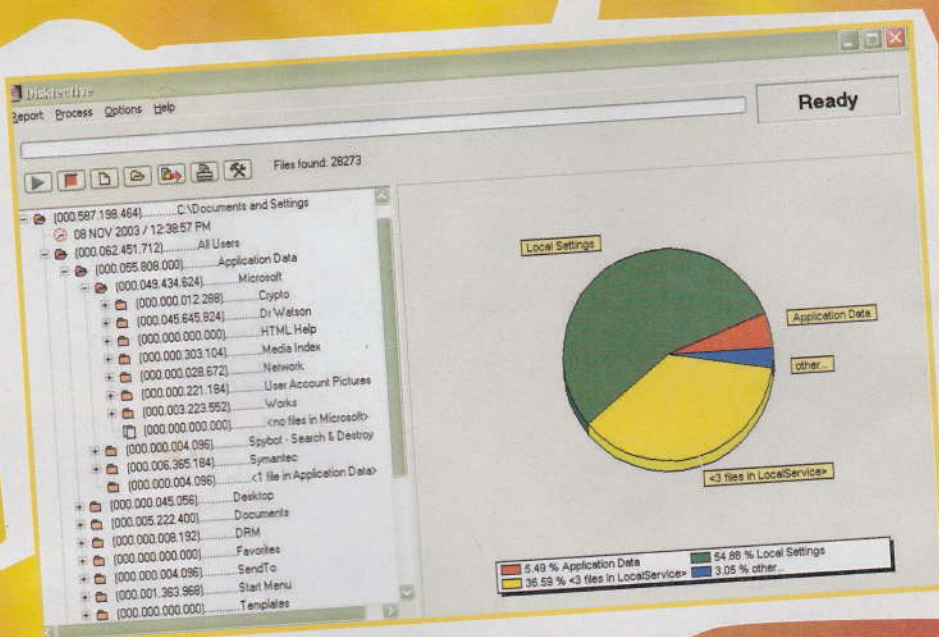
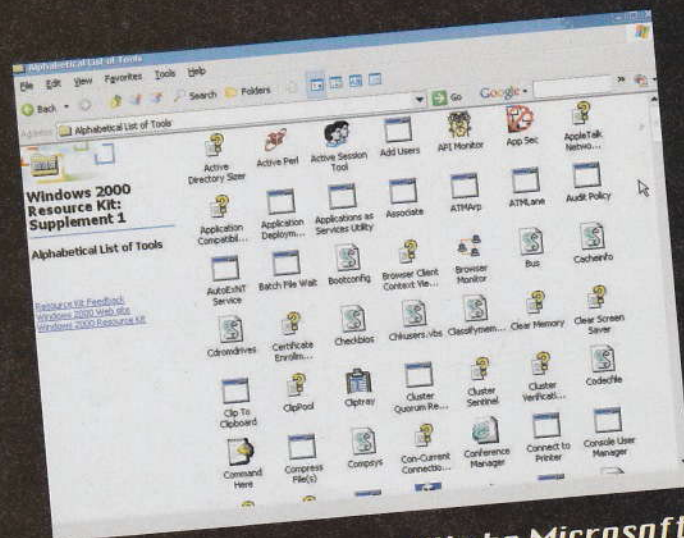
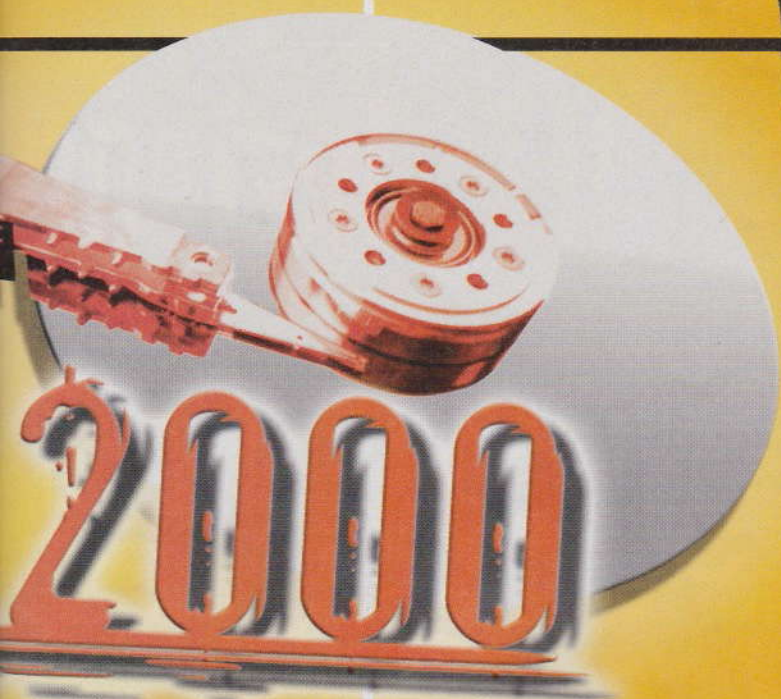
Un disco da paura con Windows

Windows mette a disposizione numerosi strumenti per ottimizzare le prestazioni del sistema. A patto di saperlo, certo

La prima cosa da fare per migliorare le prestazioni del disco è attivare tutti i contatori di attività del disco a disposizione. I contatori PhysicalDisk sono abilitati di serie nel sistema operativo e compaiono nell'interfaccia utente della console Prestazioni. Invece i contatori LogicalDisk non appaiono e dobbiamo attivarli con il comando diskperf.

Michele Campovecchio
michele_c@hackerjournal.it

IL DISCO PESA SUL SISTEMA

Un disco rigido poco efficiente danneggia l'efficienza del sistema. Per esempio, se molti programmi utilizzano intensamente in disco nello stesso momento, il throughput potrebbe raggiungere il massimo senza riuscire a soddisfare tutte le richieste e così ci sarebbe una coda di dati che attendono di arrivare a destinazione. Se lo spazio libero su disco è molto poco, i programmi non riescono a sfruttarlo al meglio delle loro possibilità e funzionano più lentamente. E così via.

Per migliorare le prestazioni di un disco rigido servono anche complicate operazioni sul registro di Windows, ma si può cominciare da programmi semplici e utili come Disktective, freeware rintracciabile a http://www.freebyte.com/disktective/.

▲ Parte del Resource Kit che Microsoft rende disponibile per Windows 2000. Alcune utility sono scaricabili gratuitamente, ma per averle tutte bisogna pagare. Rivolgersi a http://www.microsoft.com/windows 2000/techinfo/reskit/tools/default.asp.

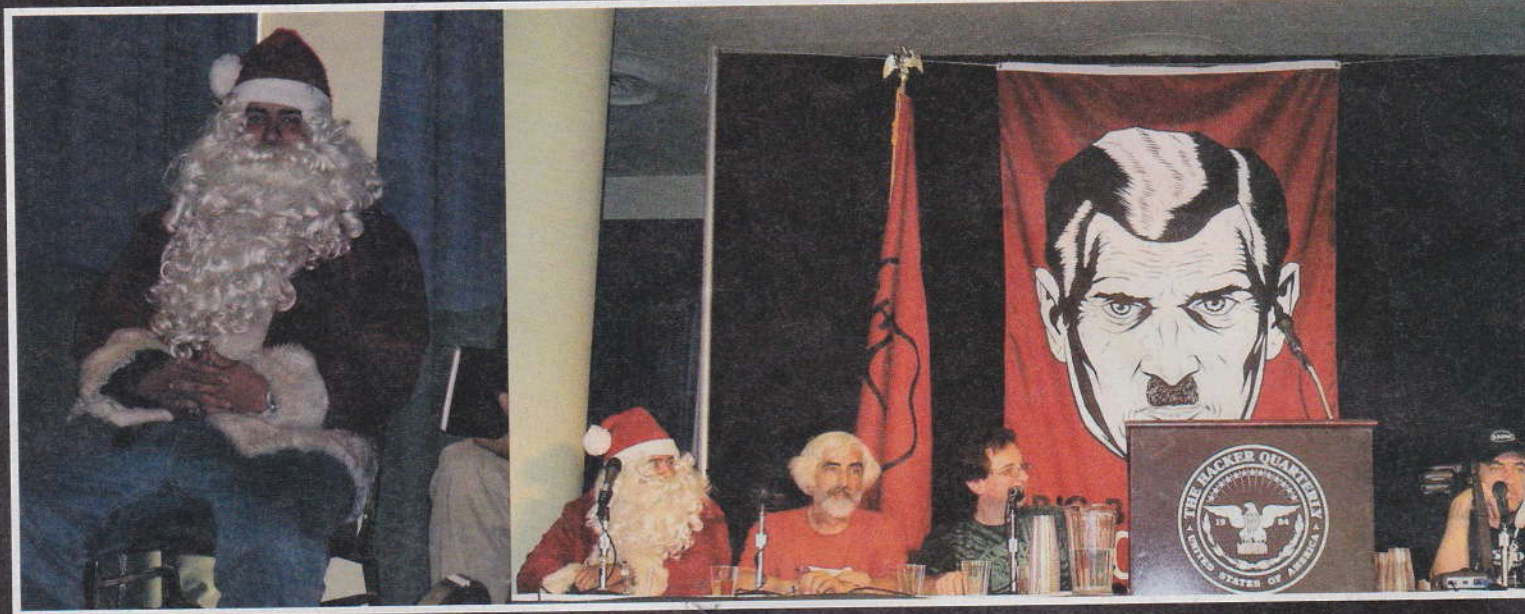
CONFIGURIAMO DISCO E FILESYSTEM PER AVERE LE MASSIME PRESTAZIONI

I*l formato migliore possibile tra quelli a disposizione per Windows 2000 è NTFS,* rispetto agli altri più affidabile e sicuro, oltre che richiesto per dischi rigidi di dimensioni elevate. Per avere il massimo delle prestazioni occorre configurare il filesystem e l'allineamento di tracce e settori. E sistemare ancora qualche parametro.

1 Disabilitare la creazione di nomi brevi. NTFS assegna ai file dei client MS-DOS e Windows 3.x nomi da otto caratteri-punto-estensione di tre caratteri. Se non abbiamo vecchi sistemi a disturbare, possiamo impostare al valore predefinito 1 la voce di registro NtfsDisable8dot3NameCreation, in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Filesystem.

2 Disabilitare l'aggiornamento del momento di accesso più recente alle directory. NTFS registra l'accesso a una directory ogni volta che il sistema la esamina per qualche motivo e questo può essere fonte di rallentamenti. Per disabilitare questo aggiornamento automatico, cambiamo al valore 1 la voce di registro NtfsDisableLastAccessUpdate, in HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Control\Filesystem. Se la voce non è già presente, aggiungiamola pure.

3 Riservare spazio appropriato per la Master File Table. Aggiungiamo al registro la voce NtfsMftZoneReservation, sotto forma di REG_DWORD in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Filesystem. In questo modo il sistema riserva spazio su disco alla tabella in modo che possa crescere senza problemi. Se sul disco i file di grandi dimensioni sono relativamente tanti, impostiamo la voce al valore 1. Se sono veramente molti, impostiamola a 4. 2 e 3 sono valori intermedi. Attenzione a verificare la situazione per valori superiori a 2, dato che il sistema potrebbe allocare alla master file table una porzione di spazio su disco esagerata.

Ingegneria SOCIALE: lezione

Questa conferenza, svoltasi allo scorso Hope a NY, mostra al lavoro le menti più famose per il Social Engineering:

La sessione invece di essere teorica o aneddotica sarà pratica e tutto l'odience (la sala è gremita, probabilmente oltre 600 persone) non aspetta altro. **Emmanuel Goldstein:** *"quando si fa Social Engineering è importante seguire regole di comportamento importanti: mai danneggiare l'obbiettivo della conversazione, perché è una persona che si fida di noi.*
Potete mentire e infatti mi presenterò come Scott Brown, ed avrò una scusa ed un obiettivo in mente. Per ottenere il risultato finale procederemo per passi ottenendo un pezzo di informazione alla volta. La nostra vittima è Taco Bell (una catena di fast food orientata al TexMex)."

Prima telefonata

EG: *"Sono Scott Brown della sede centrale, ci risulta che avete avuto un problema al registratore di cassa... Mi può dare il numero del negozio per verificare?* [Il numero del negozio è quello di affiliazione, normalmente è scritto sulle ricevute]"
... Un buco nell'acqua l'impiegato non sa il numero e non può aiutare...

Seconda telefonata

EG: "... [solita presentazione]. *posso parlare con il Supervisore? ... Ah, ciao Paul, sono Scott, Scott Brown della sede centrale, ci hanno segnalato dei problemi e dobbiamo verificare i registratori di cassa...* [chiacchiere sul quanto spesso i problemi si verificano, che non fanno più le cose come una volta, che a Pasadina il tempo e brutto ed alla fine...] *Che registratori usate lì i vecchi CR o quelli nuovi?"*
Paul: *"Boh, qui abbiamo avuto sempre i CNR"*
EG: *"CNR, 2100 o gli altri, puoi verificare Paul, per favore?"*
Paul: *"C'e' scritto 1100"*
EG: *"OK Paul, i tuoi sono a posto, grazie tanto"*

Terza telefonata

EG: "... [solita presentazione]. *posso parlare con il Supervisore? ... Ah, ciao Mike, sono Scott, Scott Brown della sede centrale e mi hanno chiesto di aggiornare i registratori di cassa, sai i vecchi CRN 1100. Sono veramente una rottura ed è bene aggiornarli altrimenti qualcuno passerà dei guai prima o poi* [notate la sottile minaccia che suona come: ora te l'ho detto se rifiuti e succede qualcosa sono affari tuoi...]"
Mike: *"Che bisogna fare?"*
EG: *"Non ti preoccupare, ci vogliono 2 minuti, facciamo 5 per buona misura: dalle 9:00 alle 9:05 non usate i registratori, sono connessi già al telefono e possiamo fare tutto da qui, basta*

in DIRETTA

Emmanuel Goldstein, Kevin Mitnik e Cheshire Catalyst!

che non facciate scontrini per quei cinque minuti; potete inserire gli ordini ma non fate scontrini..."
Mike: *"Va bene Scott allora dalle 9:00 alle 9:05. Grazie Scott* [saluti e baci]*"*
EG: *"Come vedete è stato facile e non abbiamo causato nessun danno, giusto qualche noia per 5 minuti alle nove...* [...]

Altra telefonata a BlockBuster, dove passandosi per Scott B. Ottiene il numero di telefono e l'indirizzo di una altro utente che si chiama Scott come lui ma con un altro cognome che inizia per B.
EG: *"Scott è un nome molto comune ma con l'iniziale da sola ho una possibilità molto più alta di trovare una persona che sto cercando perché tanto i nomi li ha elencati il supervisore da solo - Ora proviamo qualcosa di più difficile cerchiamo il numero di telefono del call center di Bombay della Mastercard"*

Telefonata al numero 800 della Mastercard ...

Va male: senza il numero della carta non si va avanti.
Kevin Mitnik: *"Alla America Express non serve il numero!"*
EG: *"Chiamiamo Amex...* [la voce registrata chiede il numero della carta] *battiamo 0* [la voce registrata chiede nuovamente il numero della carta] *battiamo 0* [la voce registrata chiede nuovamente il numero della carta] *battiamo 0*

[la voce dice che saremo connessi ad un operatore, la platea applaude]
Buon giorno, sono Scott Brown della MCI di New York [noto carrier telefonico americano] *e ci hanno chiamato per dei problemi sul collegamento internazionale: sembra che quando chiamano il numero 800 non arrivano a Bombay in India ma da una altra parte"*
Operatrice Amex #1 *"Qui è Manila, Filippine"*
EG: *"Ecco lo sapevo il database è tutto sotto sopra! Per risolvere il problema mi servirebbe il numero di telefono del centro di lì, dicevi Manila, vero?"*
[l'operatrice non ha il numero, ci da l'indirizzo ma il numero non lo ha proprio, ed allora ci trasferisce al supervisor.]
Supervisor Amex #1 *"[...] non ho il numero, vi passo alla sezione tecnica"*
Supervisor Amex #2 *"[...] Scott, qual'è il ticket number che avete assegnato al problema* l'odience diventa silenzioso, [questo è un momento difficile...]
EG: *"Sai Chris, stiamo cercando di risolvere il problema prima che peggiori, non è ancora grave e non gli abbiamo dato un numero ancora"*
Supervisor Amex #2: *"OK, Scott capisco, ti passo alla sezione estera"*
EG: [diretto al pubblico]: *"vedete il ticket number hanno un formato definito compagnia per compagnia, io non sapevo quante lettere e numeri dare e quindi è stato meglio dire così che sparare un numero a caso. Usate una voce annoiata ed un tono di confidenzialità come a dire - sai se apriamo il ticket poi sono guai per noi e per voi quindi se facciamo così è meglio per tutti!"*
Supervisor Amex #3,4,5,6 [passaggi su passaggi]
EG: [diretto al pubblico]: *"Talvolta è necessario fare molti passaggi"*
Supervisor Amex #7: *"Ciao Scott sono Beri* [la voce ha un chiaro accento indiano, il pubblico è in visibilio] *come ti posso aiutare?"*
EG: [ripete la storia del database e delle chiamate che arrivano in Manila invece di Bombay] *"Puoi darmi il numero diretto del call center?"*
Supervisor Amex #7: *"Certo Scott eccolo: XXX YYY XXXXXX"*
EG: *"XXX è il prefisso per l'India e YYY quello per Bombay?"*
Supervisor Amex #7: *"Giusto"*
EG: *"Grazie Beri!"*

[Fine della telefonata e tifo da stadio all'interno della sala conferenze!]

Anche gli esperti di Social Engineering hanno qualcosa da imparare. Questo ragazzo vestito da Babbo Natale si è tranquillamente seduto al palco ed ha preso la parola senza che nessuno gli chiedesse nulla o avesse da obiettare!

❏ I MAESTRI A LEZIONE

Ma i maestri di Social Engineering hanno imparato una lezione a loro volta: lo vedete quel personaggio vestito da Babbo Natale? Ora lo vedete sul parco seduto accanto a Cheshire Catalyst e parla anche al microfono! Chi era? Nessuno, solo un ragazzo che ha immaginato, giustamente, che così nessuno gli avrebbe fatto domande, un vero campione di Social Engineering! Anche i maestri ogni tanto imparano una lezione ;-)

La macchina del TEMPO

Ripercorriamo schematicamente la storia dell'informatica moderna da un punto di vista un po' particolare: quello hacker

1940 – 1970. L'era dei mainframes.

1950 J. Presper Eckert e John W. Mauchly creano l'UNIVAC, il primo computer a gestire l'input e l'informazione in formato alfanumerico.

1960 La cultura hacker contamina quella nazionale insieme ai computer. Il centro della cultyura hacker è ora il MIT e da qui all'università di Carnegie Mellon e Stanford. I più famosi hacker di questi anni sono Ed Fredkin, Brian Reid, Jim Gosling, Brian Kernighan, Dennis Ritchie, e Richard Stallman.

1969 Nasce ARPANET, la prima rete di computer che collega le università, la difesa e i laboratori di ricerca privati.

1969 L'hacker Ken Thompson crea il sistema operativo UNIX. l'hacker Dennis Ritchie crea il linguaggio di programmazione C.

1971 Un veterano della guerra del Vietnam, John Draper, scopre che il fischietto in omaggio con le scatole dei cereali Cap'n Crunch, ha una frequenza esatta di 2600 Hz. Draper, ora noto come Cap'n Crunch, costruisce una "blue box" che permette ai phreaks di effettuare telefonate gratuite. Di lì a poco il giornale Esquire pubblica un articolo "Secrets of the Little Blue box" con le istruzioni per costruire le Blue Box che consegna Cap'n Crunch alla storia, ed in breve, ai federali.

1972 Viene fondato l'InterNetworking Working Group per definire gli standard della rete che si sta sviluppando. A capo del programma c'è Vinton Cerf, il padre di Internet. Steve Wozniak e Steve Jobs incontrano Cap'n Crunch ed iniziano a vendere "blue box" ai loro compagni all'università. John Draper viene arrestato per frode telefonica. È il primo arresto e non finisce in prigione.

1973 Robert Metcalfe crea il protocollo Ethernet presso lo Xerox Palo Alto Research Center (PARC).

1975 Paul Allen and Bill Gates fondano la Microsoft (prima nota come Traf-O-Data) e scrivono il BASIC per il computer Altair.

1976 Steve Wozniak fa la prima demo dell'Apple I presso il Homebrew Computer Club. John Draper viene arrestato e condannato per frode telefonica. Questa volta Captain Crunch va in carcere, dove trascorre quattro mesi (Lompoc, Prison federale in California) tenendo corsi di phreaking per aiutare I compagni di detenzione a chiamare numeri che erano vietati dall'interno del carcere ed intercettare le radio dei sorveglianti.

1977 Apple introduce l'Apple II e Commodore introduce il computer PET. John Draper lavora per l'Apple con la matricola 13 e realizza il primo modem (mai andato in produzione perché era un blue box), che (lasciata l'Apple) Captain Crunch utilizza privatamente eseguendo decine di migliaia di telefonate in due giorni. Risultato? solita visita dei federali e immedia-

tamente dal giudice!

1978 Bill Joy ed altri sviluppano BSD, una versione del sistema operativo Unix.

1979 Hayes realizza il suo primo modem e diventa lo standard per il mercato.

1981 IBM annuncia il suo Personal Computer.

1982 Vengono fondate Sun e SGI.

1983 Il film War Games lancia una luce sinistra sul modo degli hacker e dei phreakers.

1983 I servizi segreti hanno la giurisdizione sui casi di frode con Carta di credito e computer.

1984 Due ragazzi, Lex Luthor e Phiber Optik, fondano rispettivamente Legion of Doom (LOD) e Masters of Deception (MOD). Altra figura di primo piano Erik Bloodaxe. Inizia la guerra tra LOD e MOD che si conclude con una grande retata ed un giorno di silenzio per i telefoni americani. Viene fondato in Germania il Chaos Computer Club. Negli USA viene emesso il Comprehensive Crime Control Act. Nasce The hacker magazine 2600. L'editore è Emmanuel Goldstein" (nome reale Eric Corley) che prende a prestito un personaggio da 1984 di George Orwell. Originariamente orientata ai phreaks inizia in breve a seguire I problemi degli hacker. L'Apple annuncia il Macintosh con unico storico spot durante il Super Bowl. Borland sviluppa il Turbo Pascal.

1985 L'Apple dà a Microsoft la licenza per alcune delle funzionalità dell'interfaccia grafica a finestre. Steve Jobs lascia l'Apple e fonda la NeXT.

1986 Compaq introduce il primo PC basato sulla Cpu Intel 80386.

1987 La rivista Decoder debutta in Italia. Viene creato il CERT per la sicurezza delle reti.

1988 Il primo worm: The Morris Worm. Robert T. Morris, Jr. (RTM), studente all'università di Cornell, figlio di uno degli scienziati della National Security Agency, scrive ed esegue il codice di un worm che si replica all'interno di ARPAnet per verificarne gli effetti sui sistemi UNIX. Fuori controllo il worm infetta 6.000 macchine bloccando la rete governativa ed universitaria. Morris viene cacciato da Cornell e condannato dal tribunale a tre anni di sorveglianza ed una multa di 10.000 dollari. Kevin Mitnick controlla la mail della MCI e Digital Equipment. Risultato? Kevin Mitnick è condannato ad un anno di carcere.

1990 Tim Berners-Lee inventa il World Wide Web creando HTTP ed HTML. La fine di un mito: Peter Norton vende la sua società e la sua faccia alla Symantec.

1991 Linus Torval presenta il suo progetto: Linux. È anche l'anno del virus Michelangelo che avrebbe dovuto fare una strage dei computer il 6 marzo 1992 in occasione del compleanno dell'artista. Invece non succede nulla.

1992 Microsoft rilascia Windows 3.1.

1993 È l'anno della prima Def Con, la conferenza degli hacker a Las Vegas. Il progetto originale è quello di un party di addio alle BBS ed un benvenuto ad Internet ma si trasforma in un evento annuale.

1994 Mark Andreessen e James Clark fondano Netscape.

1995 A febbraio viene arrestato Kevin Mitnick dall'FBI. L'accusa è di avere preso 20.000 numeri di carta di credito e di aver causato danni per 120 milioni di dollari impadronendosi del codice sorgente di un cellulare di Motorola e parte del codice di Solaris. Resta in carcere per quattro anni senza processo.

1997 Microsoft Internet Explorer sorpassa Netscape Communicator nel mercato dei browser.

1998 Il gruppo Cult of the Dead Cow inventa e rilascia il Trojan Back Orifice in occasione di Def Con. Linux diventa il secondo sistema operativo come tasso di crescita.

1999 Kevin Mitnick, detenuto da 1995 firma un accordo per la sua liberazione. Nasce il virus Melissa, il più diffuso virus di tutti i tempi.

2000 Kevin Mitnick esce di prigione.

2001 Microsoft viene fatta oggetto di un DOS attraverso il DNS. Il sito è su e funzionante ma gli utenti non lo possono raggiungere per quasi due giorni. Draper diventa un "white hat" hacker crea ShopIP per ripagare la società della sua precedente cattiva condotta. A luglio il programmatore russo Dmitry Sklyarov viene arrestato durante Def Con. È la prima vittima del Digital Millennium Copyright Act (DMCA). Ad agosto viene rilasciato Code Red ed a settembre Nimda, due grandi successi di tutti i tempi per velocità ed efficacia di riproduzione sulla Rete.

2002 L'amministrazione Bush crea il Dipartimento della Homeland Security.

Giugno 2002 Nasce Hacker Journal, la prima rivista hacking italiana.

◄ Commodore

► Apple

◄ modem Hayes

► Altair 8800

◄ Lo sappiamo, vero?

▲ Bill Joy

▲ John Mauchly

▲ Ken Thompson

Mozilla mette la taglia sui Bug

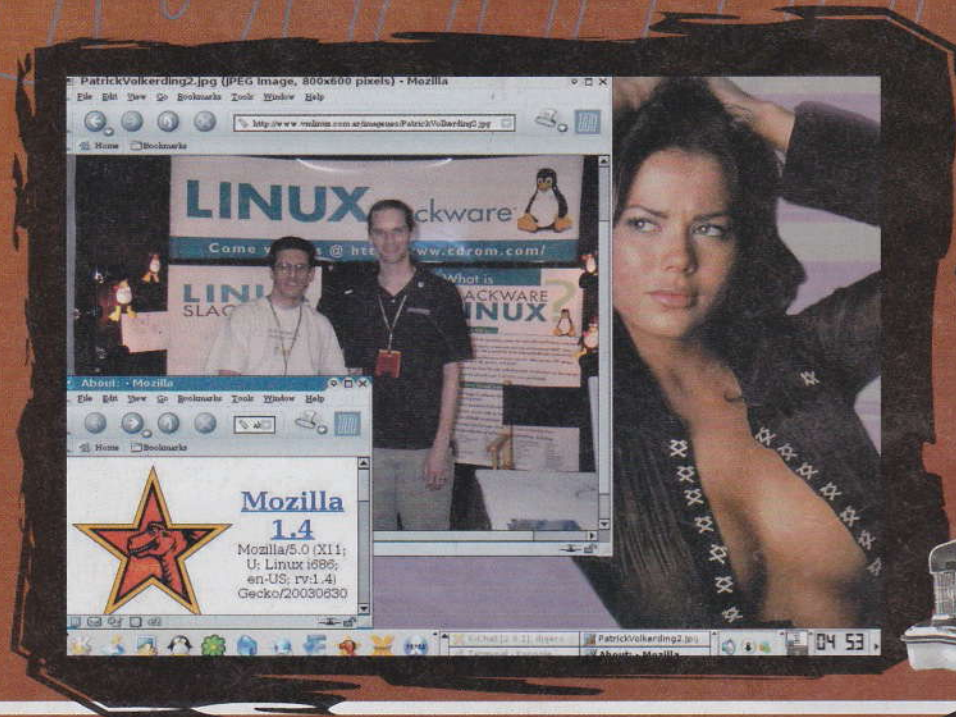
La differenza tra l'open source e Microsoft? Il primo paga per trovare i bug, la Seconda paga per trovare gli hacker

mozilla.org

Chi ha detto che con l'open source non si fanno i soldi? La Mozilla Foundation, che coordina lo sviluppo dei browser Mozilla e Firefox nonché del client email Thunderbird, ha annunciato il Security Bug Bounty Program, un'iniziativa che ricompensa con premi di 500 dollari quanti, a giudizio dello staff della Mozilla Foundation, identificano e riferiscono bug critici per la sicurezza.

Il motivo dell'iniziativa è semplice: Mozilla sta diventando importante. I bug di sicurezza in colabrodo-Explorer, il browser più usato su Internet, si susseguono in continuazione. Microsoft mette in rete patch e aggiornamenti a getto continuo,

CHI CI METTE I SOLDI

Mozilla è open source e gratis. Chi mette i soldi per compensare i cacciatori di bug? La risposta è: la comunità! I primi a contribuire sono stati l'azienda Linspire, Inc. (quelli di Lindows, http://www.linspire.com), con cinquemila dollari. Inoltre Mark Shuttleworth (http://www.markshuttleworth.com), imprenditore noto per le sue iniziative a favore del software libero, ha annunciato che raddoppierà di tasca sua tutti i contributi che arriveranno per i primi cinquemila dollari. Per il resto, il progetto conta sul contributo di tutti quelli che vogliono dare una mano. È possibile effettuare donazioni di qualsiasi entità a http://www.mozilla.org/foundation/donate.html. Ecco una risposta a chi vuole collaborare all'open source ma non ha capacità: metterci denaro!

COME GUADAGNARE 500 DOLLARI

Trovare un bug critico riproducibile nella versione più recente della Mozilla Suite, Firefox o Thunderbird. Vale la versione scaricabile in quel momento dalla pagina dei download di mozilla.org. In casi significativi vale anche per una versione development, un nightly build (le versioni rinnovate da un giorno all'altro nel corso del lavoro di sviluppo) e alcune vecchie versioni.
Per bug critico si intende un bug che permette l'esecuzione di codice malevolo sul computer della vittima o l'accesso a sue informazioni confidenziali. Non contano i bug di tipo Denial of Service, che sono molto meno gravi.
Scrivere a security@mozilla.org e descrivere il bug.
Le informazioni dettagliate si trovano a http://www.hecker.org/mozilla/bug-bounty-faq.

COME GUADAGNARE 250.000 DOLLARI

Conoscere un programmatore che potrebbe essere l'autore di un virus. Fare la spia a Microsoft.

ma non tutti lo sanno e non tutti si aggiornano all'istante (qualcuno neanche lo fa), senza contare che in ogni caso, quando arriva la patch, si è già stati vulnerabili, magari per mesi. Microsoft non è esattamente puntuale…

Così alcuni esperti hanno finalmente iniziato a spiegare pubblicamente una verità nota da tempo ai nostri lettori: si è più protetti se Explorer è spento! E, per la prima volta, Mozilla ha rosicchiato un punticino di quota di utilizzo a Explorer nelle preferenze dei navigatori di tutto il mondo.
Il problema è che Mozilla è estremamente più sicuro di Explorer, ma non è invulnerabile. Così la Mozilla Foundation ha deciso di stimolare la comunità allo scopo di individuare ed eliminare il più presto possibile i bug di sicurezza del programma.
Nel frattempo Microsoft non è stata con le mani in mano e ha messo anche lei le taglie. Non sui bug, ma sulle persone. Un fondo di cinque milioni di dollari per dare soldi a chi contribuisce a identificare l'autore di questo o quel virus. Simpatici.

Barg the Gnoll
gnoll@hackerjournal.it

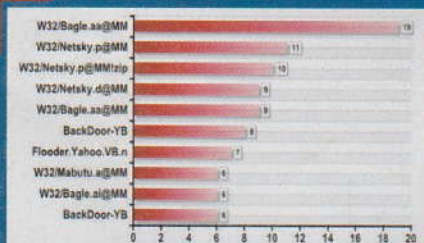
DAVIDE CONTRO GOLIA

	Internet Explorer	Mozilla
4 giugno 2004	95,73%	3,21%
6 luglio 2004	94,73%	4,05%
	-1	+0,84

Fonte: WebSideStory (http://www.websidestory.com)

BROWSER PARADE

Secondo OneStat (http://www.onestat.com) a gennaio 2004 i browser più diffusi erano questi:

1. Microsoft IE 6.0 68,1%
2. Microsoft IE 5.5 13,8%
3. Microsoft IE 5.0 11,8%
4. Mozilla 1,8%
5. Opera 7.0 0,8%
6. Microsoft IE 4.0 0,7%
7. Safari 0,48%

▲ *La top ten delle infezioni da virus nell'ultima settimana secondo Virus Total (http://www.virustotal.com). Molte delle vittime avrebbero potuto risparmiarsi l'infezione se solo non avessero usato Explorer. Se avessero usato Linux non sarebbe stato infettato assolutamente nessuno, ma questa è un'altra questione.*

Thunderbird è un'auto, un jet, un supereroe, ma anche un client email open source!

Installiamo PHP

00447793949947 00447739499948

Un sistema semplice e potente per mettere in piedi siti belli in poco tempo e con poca fatica

Pronti a installare PHP-Nuke? Qui si parla di Win XP, ma questo sistema si può installare su tutto, altri Windows, Linux, Mac OS X, altri Unix, quello che si vuole!

Questo è l'elenco dei componenti da scaricare (per Windows o XP, la versione più aggiornata che c'è):

APACHE:	http://www.apache.org
PHP:	http://www.php.net
MYSQL e MYODBC:	http://www.mysql.com
PHP-NUKE:	http://www.phpnuke.org
GALLERY:	http://jpmullan.com/galleryupdates/
NETBPM:	http://gallery.menalto.com/index.php

Primo passo: installiamo Apache

1) entriamo nel sistema come amministratori
2) installiamo Apache nel path di default
3) abilitiamolo come servizio
4) se è tutto a posto, potremo visitare con il browser l'indirizzo 127.0.0.1

Secondo passo: installiamo PHP

1) scarichiamo e scompattiamo PHP in una directory, ad esempio c:\php. Dovremmo avere una sottodirectory tipo c\:php\pdp-4.3.0-Win32 o simile
2) php4ts.dll deve essere copiato nella sottodirectory sapi, dove dovrebbero già trovarsi php4apache.dll e php4apache2.dll
3) php.ini-dist deve essere copiato nella directory di sistema, di solito c:\windows, e rinominato php.ini
4) sistemare il file di configurazione di Apache perché fornisca il supporto PHP. Il file dovrebbe essere c:\Program Files\Apache Group\Apache2\conf\httpd e bisogna aggiungergli in coda le seguenti due righe:

```
LoadModule php4_module c:/php/php-4.3.0-win32/sapi/php4apache2.dll
AddType application/x-httpd-php .php .php4
```

5) riavviare Apache.

Ora possiamo testare PHP. Dentro la

Nuke!

Come le macchine e le moto, PHP-Nuke ha il modello base e poi le versioni truccate, piene di add-on e moduli particolari per effetti altrettanto speciali. Uno di questi è PHP-Nuke Platinum, con oltre cento mod preinstallati. Chi li volesse può trovarlo a http://www.techgfx.com.

Superpersonalizzazione

directory htdocs del server Web creiamo un file prova.php4 e ci inseriamo il comando

```
<?php phpinfo(); ?>
```

Visitando la pagina prova.php4 con il browser dovrebbe apparire una serie di informazioni riguardanti PHP e il sistema. Altrimenti l'installazione non è a posto.

Terzo passo: installiamo MySQL

1) installiamo MySQL nella directory di default, c:\MySQL
2) installiamo MyODBC
3) testiamo MySQL avviando c:\mysql\bin\winmysqladmin
4) creiamo e cancelliamo un database di prova con i comandi

```
c:\mysql\bin\mysqladmin create mytestdb
c:\mysql\bin\mysqladmin drop mytestdb
```

Quarto passo: installiamo PHP-Nuke

1) scompattiamo il file zip, per esempio nella cartella c:\phpnuke
2) modifichiamo ancora il file httpd.conf di Apache in modo che punti alla directory c:\phpnuke\html. Il file dovrebbe essere C:\Program Files\Apache Group\Apache2\conf\httd.conf e il comando

```
DocumentRoot "C:/Program Files/Apache Group/Apache2/htdocs"
```

deve diventare

```
DocumentRoot "c:/phpnuke/html"
```

Inoltre dobbiamo cambiare

```
DirectoryIndex index.html index.html.var
```

che deve diventare

```
DirectoryIndex index.html index.html.var index.php
```

Ovviamente, se sappiamo che cosa fare, possiamo fare diversamente da così.

3) creiamo il database Nuke: digitiamo i comandi

```
c:\mysql\bin\mysqladmin create nuke   (crea il database)
c:\mysql\bin\mysql nuke < c:\phpnuke\sql\nuke.sql   (popola il database)
```

Questo metodo funziona meglio che visitare la pagina http://127.0.0.1/config.php, come dice la documentazione.

4) modifichiamo il file php.ini con il comando Edit php.ini:

```
[mail function]
; solo per Win32
SMTP = mail.mioprovider.net

; solo Win32
sendmail_from = account@mioprovider.net
```

PHP-Nuke Platinum ★ Recommend

The Platinum project is a package of PHP-Nuke default with over 100 preinstalled mods and security fixes all in one free package. Additional features and information can be found here.

Inclusions:
BBCode Box
Conditional Blocks
Contact Plus Module
Enhanced Downloads Module
Forum Acronyms
Forum Admin can read Private Messages
Forum Advanced Calendar
Forum Advanced Staff Page
Forum Attachment Mod
Forum Avatars
Forum Bottom Aligned Signatures
Forum Buddy List
Forum Colour Group + Staff Rank
Forum Default Avatar Guest
Forum Disable Post Count
Forum FAQ Editor
Forum Genders
Forum Keep it Moving
Forum News Advance v2.2
Forum News Advance Attach Addon
Forum News Advance Link to Profile
Forum Rank List Advanced
Forum Rank List in Admin Rank List
Forum Rules
Forum Signature Editor
Forum Smilies List
Forum Staff Page
Forum Statistics
Legal Docs Module
Members List Find User
Message Icons
Page Titles
Profile Photo
Protector System
Supporters Module
Who Viewd My Profile
User Friendly Module Admin / Block
Your Account Tweak

Security & Optimization:
Chatserv's NukePatched 2.5
Directory Protection
Mainfile Optimized
Pageheader Optimized
PHPbb 2.0.1.0
Surveys Optimized
ThemeConsole Anti-Theft
Usergroups Optimized

Redesigned:
Administration Icons
Articles Images
Default Avatar Guest Images
Downloads Images
Forum Smilies
Images Directory
Journal Images
Protector System Images
Statistics Images
Topic Icons
Your Account Images

Removed:
Addon Sample Module
All Themes Except TPlatinum
Amazon Images
AvantGo Module
Encyclopedia Module
Feedback Module
Journal Module
Non-English Language Files
News Module
WebMail Module
WebLinks Module

▲ *L'elenco dei mod nella versione customizzata Platinum di PHP-Nuke, a http://www.techgfx.com. C'è da perderci la testa!*

Quinto passo: installiamo Gallery

1) installiamo netpbm, per esempio in c:\netpbm
2) scompattiamo lo zip di Gallery nella directory Modules di phpnuke (si creerà una directory gallery)
3) usiamo i comandi seguenti in una finestra di Prompt dei comandi del DOS:

```
cd \phpnuke\html\modules\gallery
configure
```

Dal browser, scaricare la pagina http://127.0.0.1/modules/gallery/setup e, una volta finito, ritornare al prompt dei comandi DOS per dare il comando secure.

E ora siamo finalmente pronti per popolare come si deve il nostro sito made in PHP-Nuke! Magari con qualche bell'album fotografico delle vacanze (se no a che serve installare gallery?)

beth, i5b3773r@mac.com

Trovare VALORI in una ARRAY con FLASH

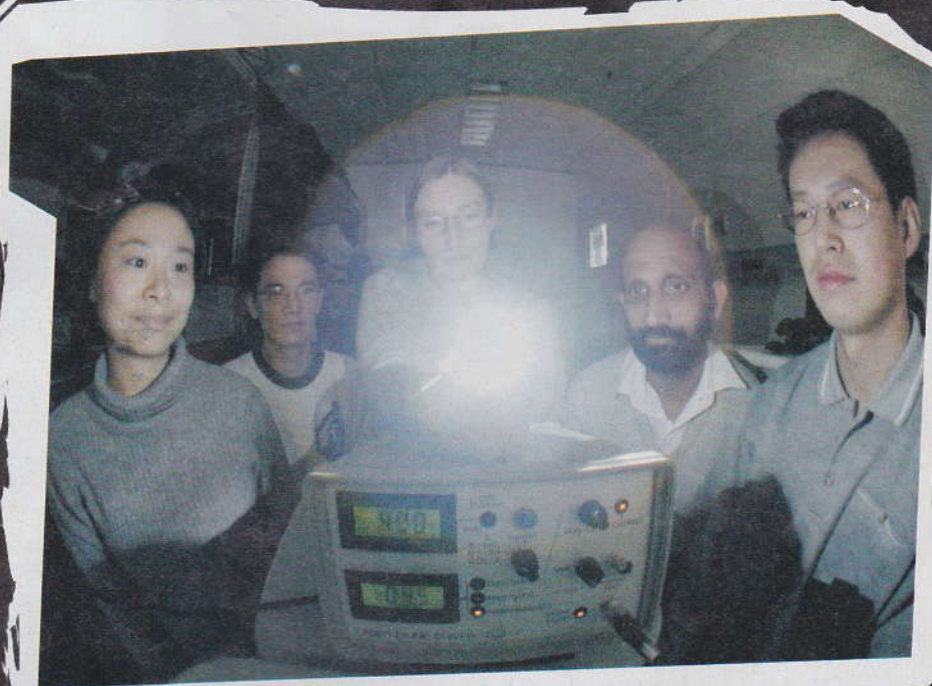
Cose da SAPERE per affrontare questo TUTORIAL

1 Conoscenze base di programmazione in Flash;

2 Che cos'è un array: un contenitore di oggetti identificati da uno o più numeri indice, secondo quante dimensioni ha l'array stesso.

lista = new Array("pippo", "topolino", "pluto", "paperino", "topolino", "minnie", "pippo"); questo è un array, in Flash. I suoi valori sono richiamabili attraverso il loro numero indice. Lanciare il movie e fare un Ctrl+Alt+V ci possiamo accorgere di come è strutturato.

```
Variable _level0.lista = [object #1,
class 'Array'] [
 0:"pippo",
 1:"topolino",
 2:"pluto",
 3:"paperino",
 4:"topolino",
 5:"minnie",
 6:"pippo"
]
```

Supponiamo che questo array ci arrivi dall'esterno e che ci serva avere una lista di valori univoci. Invece in questo array ci sono valori ripetuti, in questo caso pippo e topolino. Che fare? Dobbiamo creare qualcosa che confronti i valori dell'array, individui quelli che compaiono una volta sola e li copi in un nuovo array.

Creiamo l'array:

lista = new Array("pippo", "topolino", "pluto", "paperino", "topolino", "minnie", "pippo");

Ora creiamo l'array di appoggio, che inizialmente dovrà essere vuoto:

```
univoci = new Array();
```

ordiniamo i valori del primo array:

```
lista.sort();
```

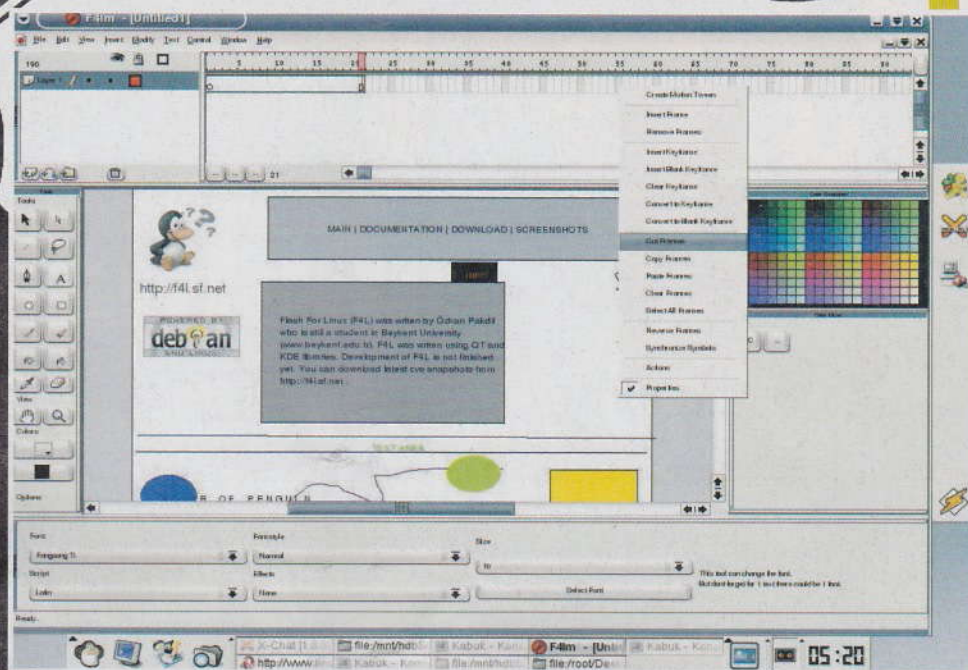
Serve un metodo che prenda il primo valore dell'array e lo confronti con il secondo, prenda il secondo e lo confronti con il terzo, poi il terzo con il quarto e così via.
Quindi prima di tutto dobbiamo sapere quanto è lungo l'array e poi programmare il ciclo.

```
for (n=0; n< lista.length; n++)
{
```

Il ciclo for crea un contatore ne ripete l'istruzione al suo interno finché n è minore della lunghezza totale dell'array (cioè il numero di valori compresi al suo interno). n servirà anche per utilizzare l'indice dell'array.

Nel ciclo inseriamo l'istruzione che confronta i valori.

```
if (lista[n]!=lista[n+1])
```

Un tutorial per fare miracoli con un software costruito per animazioni là dove sembrerebbe debba servire un database

Spiegazione: if (se) il primo valore dell'array (lista[n]) è diverso (!=) dal valore seguente (lista[n+1]) si fa qualcosa, altrimenti si passa oltre. Il qualcosa è copiare il valore confrontato dentro un nuovo array.

```
univoci.push(lista[n]);
```

Abbiamo richiamato l'array vuoto univoci e vi abbiamo inserito (push) il valore.
Questo if inserito nel ciclo for causa il confronto di tutti i valori, dato che l'indice dell'array viene incrementato dal contatore n.

Ecco tutto lo script pronto all'uso:

```
lista = new Array("pippo",
"topolino", "pluto", "paperino",
"topolino", "minnie", "pippo");
univoci = new Array();
lista.sort();
for (n=0; n< lista.length; n++) {
if (lista[n]!=lista[n+1]) {
univoci.push(lista[n]);
}
}
```

Non è difficile adattarlo alle diverse situazioni che si potranno presentare. Buon lavoro.

Warp9
http://www.warp9.it

MAL DI TESTA ?

Domanda: come facciamo a essere sicuri di aver confrontato ogni valore con tutti gli altri? Se il primo valore si confronta con il secondo, il secondo con il terzo e così via, dati i valori 1 - 2 - 3 - 4, confronteremo 1 con 2, 2 con 3 e 3 con 4, ma non di più. Qui entra in campo l'ordinamento iniziale dell'array. La lista era organizzata in questa maniera:

```
Variable _level0.lista =
[object #1, class
'Array'] [
 0:"pippo",
 1:"topolino",
 2:"pluto",
 3:"paperino",
 4:"topolino",
 5:"minnie",
 6:"pippo"
]
```

Una volta ordinata diventa

```
Variable _level0.lista =
[object #1, class
'Array'] [
 0:"minnie",
 1:"paperino",
 2:"pippo",
 3:"pippo",
 4:"pluto",
 5:"topolino",
 6:"topolino"
]
```

Basta guardare per capire che è sufficiente confrontare un valore con il suo successivo per eliminare i doppioni.

Domanda: e se i valori uguali sono tre (per esempio tre volte pippo) o più di tre? L'istruzione if era

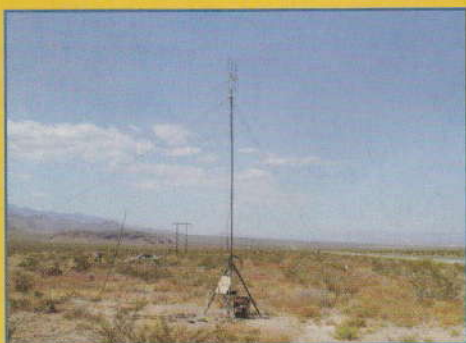
```
if (lista[n]!=lista[n+1])
```

Non confrontiamo valori uguali, ma valori diversi tramite l'operatore di confronto !=, e solo in questo caso li copiamo nella lista dei valori univoci.

Di tutti i valori uguali ne verrà sempre copiato uno solo.

WiFi Shootout!

55,1 miglia. Questa è la distanza che rappresenta il nuovo record stabilito sabato 31 luglio a circa 50 miglia da Las Vegas in occasione del secondo WiFi Shootout

STORY BOARD

▲ **A oltre ottanta chilometri di distanza da Las Vegas e con 112 gradi Fahrenheit** (44, 5 gradi centigradi) ecco la conca scelta per la seconda prova del WiFi Shootout. Secondo gli organizzatori la line dell'orizzonte, sfruttando la collina doveva essere ampiamente sufficiente: 55 miglia. Sbagliato!

▲ **Questo team di Seattle** ha installato sulla collina due antenne commerciali, una omnidirezionale ed una direzionale, tutte e due amplificate con apparti commerciali Cisco. Lì in fondo a circa 25 miglia si sono fermati i loro compagni con la postazione mobile.

▲ **Il caldo ed il vento sono stati i nemici della competizione.** Il comodo gazebo giace smontato per terra visto che il vento non ne aveva permesso l'installazione sulla collina. La copertura dei cellulari al centro del deserto è incedibile: questo vecchi telefono analogico funziona, il mio GSM è morto trenta miglia prima.

◄ **"Ci sono voluti quattordici viaggi** da laggiù per portare tutta l'attrezzatura qua sulla collina; ieri eravamo così stanchi che ci siamo addormentati prima che arrivassero le pizze e ci siamo svegliati questa mattina ancora vestiti" Certo che se un hacker non viene svegliato dalla pizza allora deve essere proprio morto ...

◄ **L'antenna fissa guarda a 55,1 miglia** su una lingua di terra in fondo ad uno sterrato, sulle montagne dall'altro lato della conca, dove si sono avventurati gli altri con il carrello. Team P.A.D (Parabolic Antenna Designer) è il nome che il gruppo ha scelto per la competizione.

▲ **Queste due ragazze vengono da Washington DC.** Loro hanno vinto il premio per l'antenna più innovativa, realizzata con quella plastica alluminiata che si usa per tenere il calore fuori dall'abitacolo delle macchine. Purtroppo non hanno fatto i conti con il calore infernale del deserto e la struttura dell'antenna ha ceduto obbligandole a tenere l'antenna aperta con le mani.
Poco più di un chilometro la distanza coperta senza amplificazione.

Tre ragazzi (o meglio quattro, incluso uno che non è potuto venire in Nevada) dell'Ohio di meno di 19 anni si sono così aggiudicati il premio Uber Hacker che da loro accesso a vita alle prossime DefCon, costruendo una coppia di antenne paraboliche di quasi tre metri di diametro.
Il record per sistemi amplificati è stato stabilito nel 2003 da Alvarion e la Swedish Space Corporation che hanno stabilito il contatto con un pallone aerostatico a oltre 310 chilometri di distanza. I problemi della curvatura terrestre e la stessa atmosfera fanno sì che il collegamento con il pallone sia molto più semplice che effettuato tra due stazioni a terra. La stima della massima distanza possibile dovrebbe essere comunque di circa 400 chilometri.
Ma i ragazzi dell'Ohio, raggiunta la massima distanza che la località permetteva, hanno notato una insolita qualità del collegamento ed allora hanno avuto l'insana e balzana idea di eliminare l'amplificatore, tanto per farsi quattro risate ed invece: miracolo! Nuovo record del mondo per una connessione non amplificata: 88,67 km.

Sono partiti a caccia di connessioni non protette. Sono arrivati qui

È interessante notare cosa ha portato i ragazzi a DefCon e a partecipare al secondo WiFi Shootout. Il loro progetto originale era di andare in giro per Cincinnati alla ricerca di connessioni WiFi non protette. Identificata la connessione contattavano l'utente e si offrivano di proteggerla. I risultati di questa attività sono stati interessanti, specialmente quando le persone, insospettite dalla richiesta chiamavano la polizia o li cacciavano in malo modo.
A questo punto dovevano trovare una utilizzazione per le parabole ed eccoli qui a guidare per duemila miglia con una antenna di tre metri (due metri ed 89 centimetri per la precisione) su un carrello...

Silvio de Pecher
http://www.wifi-shootout.com/

▲ **Questi sono i vincitori** dello scorso anno ASLRulz. Il loro record di 35,2 miglia è stato polverizzato ed inoltre anche loro non hanno fatto i conti con la fornace del deserto: la pistola a colla qui non funziona ed non riescono ad attaccare la rete ai supporti. Alla fine useranno delle fascette a strappo e non faranno molta strada.

▲ **Team P.A.D** (Parabolic Antenna Designer). Da sinistra a destra Justin Rigling, Andy Meng e Ben Corrado ritirano la messe di premi riservati ai vincitori delle categorie per antenne autocostruite amplificate e non.

▼ **Il carrello con il disco.** Immaginate di percorrere oltre 2000 miglia con questo coso! Ma adesso immaginate di trovarvelo parcheggiato davanti a casa con un ragazzo che farfuglia qualcosa su problemi alla vostra connessione WiFi; non chiamereste la polizia anche voi?

▼ **Per il ritorno il team sceglie di smontare tutta l'attrezzatura.** Li attendono quasi due giorni viaggio prima di arrivare a casa. Potete vedere le strutture in ferro necessarie a supportare l'antenna ed immaginare la fatica fatta per portarle sulla collina con 40 gradi sotto il sole!

◄ **Le frequenze del WiFi** sono MOLTO vicine alla frequenza di risonanza dell'acqua. Specialmente gli occhi possono risentire delle conseguenze di manovre sbagliate o azzardate con antenne amplificate ad alto guadagno.

NON ESISTONO file INVISIBILI in WINDOWS

Abbiamo già scritto che i file nascosti di Windows a cui bisogna fare più attenzione sono gli **index.dat**, archivi che contengono riferimenti a cronologia, cache e cookie generati dall'uso del browser. Microsoft fa del suo peggio per nasconderli e noi li raggiungiamo ugualmente. Cancellare in modo consueto cronologia e cache non li cancella tutti e quindi una registrazione dei nostri movimenti esistente anche quando pensiamo il contrario.

▲ *Se non vogliamo passare da DOS possiamo affidarci a programmi fatti apposta, come U-Wipe*

Per essere sicuri che tutto sia a posto, procediamo in questo modo. Lanciamo una finestra di Prompt dei comandi DOS e digitiamo il comando

```
c:\windows\explorer /e,c:\windows\tempor~1\content.ie5\
```

Le voci alfanumeriche che appaiono sono i nomi delle cartelle che contengono la cache. Di solito il contenuto di queste cartelle è invisibile nell'interfaccia grafica, inoltre certi file sono protetti dalla cancellazione, quindi – dopo avere preso nota dei nomi alfanumerici delle car-

Programmi di cancellazione totale

Quando buttiamo un file nel cestino, è tutt'altro che veramente cancellato. Questi programmi aiutano a completare l'opera in modo che il file cancellato sia il più possibile distrutto e irrecuperabile. Un professionista motivato può recuperare dati persino da tracce del disco rigido su cui si è riscritto sette volte!

BCWipe (shareware)
http://www.bcwipe.com
Wipe 2.06 (freeware)
http://www.geocities.com/jadoxa/delenxrd/
PGP (freeware)
http://www.pgpi.org (nei PGP Tools)
Evidence Eliminator (commerciale)
http://www.evidence-eliminator.com

Cancellare cronologia e cache non cancella tutti gli index.dat; alcuni restano. Risultato: una registrazione dei nostri movimenti esistente anche quando pensiamo di avere eliminato tutto.

▲ *BCWipe: cancella i dati come farebbe il Department of Defense americano. Hai detto niente!*

telle – bisogna riavviare in modalità MS-DOS. Riavviato il computer, i comandi sono

```
CD\WINDOWS\TEMPOR~1\CONTENT.IE5
CD nomecartella
```

Nomecartella sarà il nome della prima cartella di cui abbiamo preso nota.

```
DIR/P
```

Questi sono i file di cache che occupano spazio sul nostro hard disk e, peggio, portano insicurezza sulla privacy dei dati. Una cosa interessante di questi file è che spesso contengono messaggi di posta anche molto vecchi del nostro account Hotmail (se ne abbiamo uno, certo). Per vederli bisogna copiare i file in un'altra cartella.

Ah: sono file di cache. È possibile che, cancellandoli, certe pagine richiederanno più tempo di scaricamento quando ci torniamo sopra nel Web. I file di cache in sé non hanno niente di sbagliato. È quando intendiamo cancellarli, e Microsoft, disobbedisce, che non vanno bene. Ora digitiamo

```
CD\WINDOWS\TEMPOR~1\CONTENT.IE5
EDIT /75 INDEX.DAT
```

Apparirà uno schermo blu pieno di caratteri apparentemente senza gran senso. Scorriamo il file fino a quando non appare una serie di URL. Sono tutti siti che abbiamo visitato. Si vede spesso anche testo che abbiamo digitato in un motore di ricerca. Per uscire dalla schermata blu usiamo il menu File -> Exit. Se DOS non supporta il mouse, come è probabile, usiamo Alt per fare scendere il menu e poi aiutiamoci con i tasti freccia. Tornati in DOS, digitiamo

```
C:\WINDOWS\SMARTDRV
CD\WINDOWS\TEMPOR~1
DELTREE/Y TEMPOR~1
```

Al posto di CD\WINDOWS\TEMPOR~1 va, ovviamente, il giusto comando di cambio directory. La cancellazione impiegherà probabilmente molto tempo. Per cancellare il contenuto della cartella della Cronologia digitiamo

```
CD\WINDOWS\HISTORY\HISTORY.IE5
EDIT /75 INDEX.DAT
```

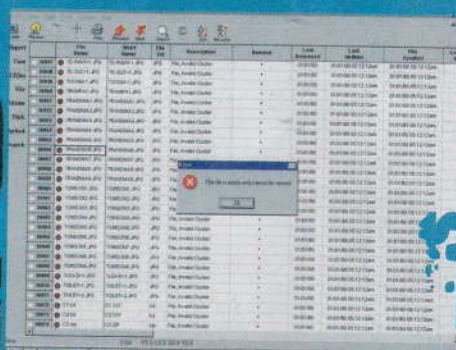
Altro elenco di URL che abbiamo visitato. Per liberarcene,

```
CD\WINDOWS\HISTORY
```

Sono da cancellare tutti i file in formato MMxxxx.dat. Altro giro:

```
CD\WINDOWS\HISTORY\HISTORY.IE5
CD MSHIST~1
EDIT /75 INDEX.DAT
```

Altri URL. Probabilmente esiste più di una cartella MSHIST~x. Ripetiamo la procedura per ciascuna. Quando ne abbiamo abbastanza, dimentichiamoci di loro con

```
CD\WINDOWS
DELTREE/Y HISTORY
```

◄ *Un programma come Evidence Eliminator costa molto, ma il suo lavoro è professionale come quello di un chirurgo di fama.*

L'anonimato in irc può essere raggiunto in vari modi e con vari livelli di sicurezza. Gli strumenti più utilizzati sono i proxy, i socks e l'ipv6, che al momento sembra il più affidabile; ma esistono metodi di anonimizzazione molto più semplici da utilizzare, anche per i meno esperti. Uno di questi è l'utilizzo di webchat che crittano l'host. Ma l'algoritmo di crittazione è veramente sicuro? O con un paio di calcoli si può risalire all'indirizzo ip dell'utente?

Proviamo

Facciamo alcune prove utilizzando diverse webchat. Useremo un paio di quelle più utilizzate dagli utenti, come

```
http://webchat.xs4all.nl e
http://chat.ircnet.org
```

Per conoscere l'indirizzo ip di un utente su irc basta digitare il comando

```
/dns nickutente
```

Interrogando così il dns, nel primo caso abbiamo la risposta:

```
Dns resolved webchat.xs4all.nl to
194.109.129.221
```

Nel secondo caso:

```
Dns resolved chat.ircnet.org to
195.40.122.125
```

Quindi il dns non fa altro che sostituire l'host dell'utente con l'host della webchat.

IRCnet Login (Main)

Nickname: Spod10522
Channel: #Beginner
Advanced.. Login

▲ *Per partecipare a una chat inseriamo l'identificativo e il canale a cui vogliamo collegarci.*

Però qualche informazione relativa all'ip sorgente deve pur esserci da qualche parte.
Proviamo a utilizzare il comando

```
/whois nickutente
```

che ci dà informazioni anche riguardo all'ident e al full name.
Le rispettive risposte sono:

```
User1 is
525415d3@webchat.xs4all.nl *
[525415d3]
```

```
User2 is
~525415d3@chat.ircnet.org *
[525415d3]
```

Analizzando la prima stringa si nota che l'ident e il full name sono identici, e anche nella seconda: il nostro ip in questo caso è 82.84.21.211.

Ora cambiamo ip ricollegandoci e interroghiamo nuovamente il whois, questa volta il nostro ip è 82.84.80.62:

```
User1 is
5254503E@webchat.xs4all.nl *
[5254503E]
```

```
User2 is
~5254503E@chat.ircnet.org *
[5254503E]
```

L'ident e il full name sono cambiati: quindi probabilmente è proprio lì che sono inserite le informazioni riguardanti il nostro ip sorgente.
Confrontiamo il primo ip con il primo ident e il secondo ip con il secondo ident:

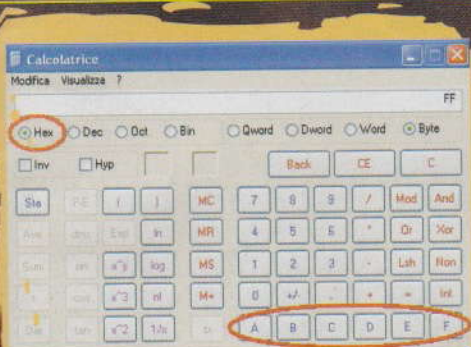
```
Ip1: 82.84.21.211
Id1: 52 54 15 d3
```

CGI:IRC Login

Nickname: XS4-0874
Channel: #worldchat
Advanced.. Login

▲ *Quale indirizzo IP si cela dietro questo utente? E' possibile scoprirlo con qualche trucco di conversione.*

Un metodo per rimanere anonimi sulle chat è quello di crittare l'host. Ma è poi così sicuro?

IP nelle

▲ **Con la calcolatrice di Windows possiamo fare calcoli e trasformare i numeri anche in esadecimale.**

Ip2: 82.84.80.62
Id2: 52 54 50 3

Ciò che si nota immediatamente è che innanzitutto in due istanze diverse numeri uguali vengono crittati allo stesso modo. Infatti notiamo i primi due blocchi dei due ip e i rispettivi blocchi negli ident:

82=52 e 84=54

Ora connettiamoci con altri ip per fare altri confronti:

Ip3: 82.84.10.26
Id3: 52 54 0a 1A

Ip4: 80.183.120.219
Id4: 50 B7 78 DB

Negli ident c'è qualcosa di molto importante, che ci potrebbe far arrivare alla chiave per giungere all'ip sorgente. Infatti l'ident non è costituito solo da numeri, ma anche da lettere e le lettere comparse nelle prove sono : A B D E

Queste lettere e in particolare questa uguaglianza 10=0a che si presenta nel terzo blocco del terzo ip ci fanno subito pensare al codice esadecimale, che è composto dalle seguenti cifre :

0 1 2 3 4 5 6 7 8 9 A B C D E F.

Per trasformare un numero da esadecimale in decimale bisogna scomporre tale numero in unità singole, poi da destra verso sinistra si moltiplica il valore dell'unità per 16 elevato alla posizione dell'unità stessa (ricordandoci che A=10 B=11 C=12 D=13 E=14 F=15); la prima posizione a partire da destra assume il valore 0. Infine si sommano i valori risultanti dalle moltiplicazioni e il risultato ci restituirà il numero decimale. Proviamo a trasformare il primo Id da decimale in esadecimale, considerando singolarmente i numeri dei quattro blocchi:

```
Hex=52  5*(16^1) + 2*(16^0) = 82
Hex=54  5*(16^1) + 4*(16^0) = 84
Hex=15  1*(16^1) + 5*(16^0) = 21
Hex=d3  d*(16^1) + 3*(16^0) = 211
```

Mettendo in serie i quattro numeri decimali ricavati abbiamo 82.84.21.211 che sarebbe l'ip corrispondente al primo id. Ecco scoperto il "trucco".

Reno [WONNER]
Imp3r4tor@hackerjournal.it

La conversione esadecimale-decimale

Con la tabella sottostante possiamo trasformare le cifre esadecimali in decimali e viceversa. Naturalmente a noi interessano solo le cifre decimali che vanno da 0 a 255 poiché un blocco dell'ip non può andare oltre il valore 255 in quanto è formato da 1 byte, che può assumere massimo 2^8 valori, cioè 256 valori.

Dec.	Hex.	Dec.	Hex.	Dec.	Hex.	Dec.	Hex.	Dec.	Hex.
0	0	51	33	102	66	153	99	204	CC
1	1	52	34	103	67	154	9A	205	CD
2	2	53	35	104	68	155	9B	206	CE
3	3	54	36	105	69	156	9C	207	CF
4	4	55	37	106	6A	157	9D	208	D0
5	5	56	38	107	6B	158	9E	209	D1
6	6	57	39	108	6C	159	9F	210	D2
7	7	58	3A	109	6D	160	A0	211	D3
8	8	59	3B	110	6E	161	A1	212	D4
9	9	60	3C	111	6F	162	A2	213	D5
10	A	61	3D	112	70	163	A3	214	D6
11	B	62	3E	113	71	164	A4	215	D7
12	C	63	3F	114	72	165	A5	216	D8
13	D	64	40	115	73	166	A6	217	D9
14	E	65	41	116	74	167	A7	218	DA
15	F	66	42	117	75	168	A8	219	DB
16	10	67	43	118	76	169	A9	220	DC
17	11	68	44	119	77	170	AA	221	DD
18	12	69	45	120	78	171	AB	222	DE
19	13	70	46	121	79	172	AC	223	DF
20	14	71	47	122	7A	173	AD	224	E0
21	15	72	48	123	7B	174	AE	225	E1
22	16	73	49	124	7C	175	AF	226	E2
23	17	74	4A	125	7D	176	B0	227	E3
24	18	75	4B	126	7E	177	B1	228	E4
25	19	76	4C	127	7F	178	B2	229	E5
26	1A	77	4D	128	80	179	B3	230	E6
27	1B	78	4E	129	81	180	B4	231	E7
28	1C	79	4F	130	82	181	B5	232	E8
29	1D	80	50	131	83	182	B6	233	E9
30	1E	81	51	132	84	183	B7	234	EA
31	1F	82	52	133	85	184	B8	235	EB
32	20	83	53	134	86	185	B9	236	EC
33	21	84	54	135	87	186	BA	237	ED
34	22	85	55	136	88	187	BB	238	EE
35	23	86	56	137	89	188	BC	239	EF
36	24	87	57	138	8A	189	BD	240	F0
37	25	88	58	139	8B	190	BE	241	F1
38	26	89	59	140	8C	191	BF	242	F2
39	27	90	5A	141	8D	192	C0	243	F3
40	28	91	5B	142	8E	193	C1	244	F4
41	29	92	5C	143	8F	194	C2	245	F5
42	2A	93	5D	144	90	195	C3	246	F6
43	2B	94	5E	145	91	196	C4	247	F7
44	2C	95	5F	146	92	197	C5	248	F8
45	2D	96	60	147	93	198	C6	249	F9
46	2E	97	61	148	94	199	C7	250	FA
47	2F	98	62	149	95	200	C8	251	FB
48	30	99	63	150	96	201	C9	252	FC
49	31	100	64	151	97	202	CA	253	FD
50	32	101	65	152	98	203	CB	254	FE
								255	FF

CODICE OFFUSCATO all'ITALIANA

Avevamo lanciato tempo fa una sfida per chi volesse spedirci programmi tanto ingegnosi nell'esito quanto curiosi nell'aspetto. Ecco una delle migliori risposte pervenute!

Questo codice obfuscated è stato scritto in Perl, e mostra un tux che rimbalza sui bordi del terminale. Possiamo trovarlo a http://perlmonks.org/index.pl?node_id=375376.
La forma è stata ottenuta mediante Banner, un programmino che possiamo trovare, nella maggior parte delle distro Linux, in /usr/games/banner.
Il codice è stato applicato mediante un software creato da me, mask.pl, che in principio serviva a "spalmare" il contenuto di un file di testo su un altro file di testo che conteneva l'immagine, e stamparne il risultato; l'ho trasformato poi, con pochi ritocchi, in un obfu generator.
Possiamo trovare anche questo sul sito Perlmonks, cercando in http://perlmonks.org/index.pl?node=Code%20Catacombs nella sezione Miscellaneous.
JumpingTux non funzionerà sotto Windows, perché i codici di escape usati per le coordinate del pinguino funzionano solo sotto shell Unix.
Possiamo comunque far girare il codice sotto cygwin.
Un altro avvertimento: se usiamo Konsole la combinazione Ctrl-Z non sortirà alcun effetto, quindi per chiudere il programma dovremo chiudere necessariamente anche il terminale.
Consigliamo perciò di utilizzare xterm o rxvt, come terminale, al posto di Konsole.
Procuriamoci anche l'ultima versione del comando sleep, perché le versioni un po' più vecchie non supportano i numeri a virgola mobile: la frequenza di aggiornamento è di 20 frame per secondo (0,05 secondi di sleep), e portarla a un frame per secondo darebbe un risultato davvero noioso.

▲ Jumping Tux in azione!

Purtroppo anche gli scrittori di virus e codice malevolo tendono a offuscare il loro codice appena possono.

Titolo da scrivere

>> CYGWIN

Nome combinazione di Cygnus (gli sviluppatori originali erano di Cygnus Solutions) e Windows, è una raccolta open source di strumenti che consentono di compilare ed eseguire programmi Unix o Linux su Windows dentro una interfaccia simile a quella di Linux.

>> DISTRO

Contrazione di distribution, indica un insieme specifico di variante di Linux completa di programmi a disposizione. Tipiche distro sono Mandrake, Red Hat, Debian eccetera.

>> OBFUSCATED CODE

Letteralmente codice offuscato: un programma completamente funzionante, il cui codice è disposto a formare un disegno; ciò rende poco leggibile, appunto offuscato, il codice.

>> TUX

Pinguino simbolo di Linux e del software libero in generale.
Il nome viene da tuxedo, lo smoking anglosassone.

OBFUSCATION IN PERL

Se vogliamo dare un'occhiata ad altre opere di obfuscation in Perl, possiamo trovare molte creazioni interessanti sul sito http://perlmonks.org/ nella sezione Obfuscation, alcune delle quali sono già state segnalate nell'articolo di Michele Campovecchio sul numero 48 di HJ.

Adesso siamo pronti a lanciare il programma; apriamo una shell e digitiamo:

```
$ chmod +x jumpingtux.pl
```

per abilitare i permessi di esecuzione del programma, quindi

```
$ echo "$COLUMNS,$LINES"
80,24
$ ./jumpingtux.pl 80 24
```

o, più semplicemente:

```
$ ./jumpingtux.pl $COLUMNS $LINES
```

per avviare il programmino.

Il BRIVIDO della COMPETIZIONE offuscata

Gli appassionati di codice offuscato hanno anche il loro campionato mondiale annuale: su http://www.de.ioccc.org/main.html si possono scoprire le regole e anche divertirsi a vedere i programmi in gara.

IOCCC
The International Obfuscated C Code Contest
People who have won
[The Judges | IOCCC home page | How to enter | FAQ | IOCCC news | People who have won | Winning entries]
People who have won the IOCCC

$COLUMNS e $LINES sono le variabili che contengono le dimensioni della finestra del terminale: vanno passate come argomento al programma cosicché possa coprire correttamente tutta l'area del terminale.

Se non vengono passate, allora il programma non avrà alcun effetto e si tornerà al prompt della shell.

Speriamo che questo lavoro di obfuscation sia di gradimento per i lettori. Speriamo anche di ricevere quali sono le opinioni di tutti in merito!

—(X-3mE'89)—

1001000110001100011010

Jumping Tux!

Il listato si pauò vedere anche alla pagina http://perlmonks.org/index.pl?node_id=375376.

DOPPIO OTTIME

ELIMINARE LE PAROLE DOPPIE: LO SAPPIAMO FARE! PROCLAMIAMO SENZA INDUGIO AD ANNUNCIARE I CYBERENIGMISTI CHE HANNO RISPOSTO ALLA NOSTRA SFIDA.

IL CYBERENIGMA ORIGINALE

PER TUTTI: trovare un sistema che consenta di effettuare in unico passaggio ricerche e sostituzioni su più file HTML in più directory nidificate.
PER ESPERTI: risolvere il problema precedente e eliminare le parole doppie anche una parola sta a fine riga e l'altra all'inizio della riga dopo.
PER GENI: risolvere i due problemi precedenti e trovare le parole doppie senza distinguere tra maiuscole e minuscole e senza badare agli spazi bianchi tra le parole.
PER SUPER HACKER: risolvere i tre problemi precedenti e trovare le parole doppie anche se sono separate da tag HTML.

LA RISPOSTA

NON ESISTE! O meglio non ne esiste una sola, ci sono infatti tanti modo diversi per arrivare al risultato, come bene ha capito chi ci ha scritto.
Non per fare il saggio dei poveri, ma questo si può applicare ad un sacco di situazioni nella nostra vita...

SÌ, MA...

Carissima redazione di HJ, rispondo alla domanda da super-hacker: io saprei farlo.

Saluti, avktrom

D'accordo... ma che cosa? :-)

==(X-3ME'89)==, FLEX E UN PO' DI SCRIPTING BOURNE:
Superhacker!
Bravissimo perché sei anche il primo arrivato e anche per ricordare la GPL.

DANIELE MIDI, PERL:
Superhacker!
Complimenti a te per la costanza e la precisione, invece.

TEOREMA55, VBSCRIPT:
Superhacker!
L'output del suo programma è visibile a http://www.larianaweb.com/cyberenigmi/Cyber_doppio_colpo/doppio.asp.

\`KAZAMA\`, MIRCSCRIPTING:
Superhacker! (a tredici anni)!
Mandaci tutto e l'articolo... perché non lo scrivi tu? Lo pubblichiamo volentieri!

VIKINGO211, JAVA:
Genio!
Hai ragione... ci stiamo lavorando. Complimenti per la compattezza del codice!

[NUANDA], VB6:
Genio!
Grazie del suggerimento, ci pensiamo.

FOX91:
Per tutti!
Dici che lo fa bene anche Word... ma facci vedere come!

TANK:
Per tutti!
Ha trovato un ottimo programma shareware per la bisogna su Internet, Advanced Find and Replace di Abacre, a http://www.vknoware.com/afr/index.htm.

Le risposte sono state pochine: eravamo tutti in vacanza o la sfida era troppo difficile? :-) Nessun problema: ci ritroviamo tutti tra due settimane con un altro Cyberenigma!

Barg the Gnoll
gnoll@hackerjournal.it

COLPO, RISPOSTE

▲ *Per risolvere problemi come questo sono stati scritti fior di programmi apposta, come Advanced Find and Replace, a http://www.vknoware.com/afr/index.htm.*

◄ *I programmi dei cyberenigmisti hanno anche l'interfaccia grafica, ora! Qui esegue validamente in Java Vikingo211.*

==(X-3ME'89)== IN FLEX E BOURNE SHELL

Per risolvere il Cyberenigma pubblicato sul numero 56 ho scritto un parser con flex unito ad un po' di scripting Bourne. Per compilare il file, lanciare i seguenti comandi:

```
$ flex html_err.yy
$ gcc lex.yy.c -o html_err -lfl
```

Per processare le pagine HTML, posizionarsi nella directory root del server (quella contenente le directory con i file HTML), copiarci i due file e lanciare lo script correct.sh più in basso.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~ File html_err.yy          ~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

/////////////////////////////////////////////

/***********************************************/
        /* html_err v0.1_alpha by X-3mE'89        */
        /* liberamente modificabile e ridistribuibile */
        /* secondo i termini della GNU General Public
*/
        /* License
*/

/***********************************************/

/////////////////////////////////////////////
        /* serve l'header string.h per strcasecmp e
strcpy */
%{
#include <string.h>
%}
        /* per il confronto tra la stringa vecchia */
        /* e quella nuova                    */
        char old[4096];

        /* Tutto quello che non e' tag */
STRING  [a-zA-Z0-9\(\)\&\%$£\^\[\]\@\#]+

        /* %pointer = yytext e' un puntatore */
%pointer

%%
        /* lascia i tag cosi' come sono */
"<"[/]?\s*{STRING}\s*[/]?">"      printf("%s",yytext);
        /* processa le stringhe */
{STRING}
if(strcasecmp(old,yytext)!=0) {

printf("%s",yytext);

strcpy(old,yytext);
                                                }
%%

int main(int argc, char **argv)
{
        /* controlla l'esistenza degli arg */
        if(argc>0) yyin=fopen(argv[1],"r");
        else exit(1);
        /* controlla l'esistenza dei file */
        if(!yyin) exit(1);
        /* parsa il file */
        yylex();
        return 0;
}
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~ File correct.sh           ~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
#!/bin/bash
for i in `find -iname '*.html'`;
do
        htmlparse ${i}>${i}_;
        mv ${i}_ ${i};
done;
```

>>NEXT CYBERENIGMA

IL PROSSIMO NUMERO IN EDICOLA IL 7 ottobre 2004!

CYBERENIGMA

Posta split!

Benvenuto nel magico mondo della crittografia visiva! Serve a spedire messaggi cifrati a un amico senza che lui debba conoscere una chiave.

Funziona così: scriviamo il messaggio, lo cifriamo in modo visivo e lo spediamo diviso in due, in due invii diversi. Al nostro destinatario, ricevute le due metà, basterà effettuare una semplice operazione.

✪ **Per tutti:** Quale operazione? Qui sotto c'è un messaggio per tutti i lettori di Hacker Journal. Riesci a leggerlo? Ricorda: il messaggio è uno, diviso in due parti...

✪✪ **Per esperti:** Quando hai risolto il problema precedente, riesci a pensare a un altro metodo visuale di cifratura per mandare messaggi senza che il destinatario debba conoscere una chiave?

✪✪✪ **Per geni:** Oltre a risolvere i problemi precedenti, riesci a trovare un sito Web che effettua automaticamente la cifratura?

✪✪✪✪ **Per super hacker:** Dopo avere risolto gli altri problemi, riesci a scrivere un programma che cifra visualmente un messaggio dato, possibilmente dietro inserimento di una passphrase di cifratura?

Per i disperati: Scrivi a guestbook@hackerjournal.it, con subject aiutino, e poni una domanda precisa. Ti arriverà una risposta fumosa... ma utile. :-)

le risposte a:

guestbook@hackerjournal.it